Brittany Powell
Joe Gutmann
Juan Miguel Cano
Nathalie Abdallah
Rodolfo Gonzalez
Scotty Jokon

PRIME TIME Defenders

Blue Team – 1

How to utilize Splunk for cybersecurity defense effectively:

1. Data Collection

- **Configure Data Inputs**:
    - **AWS CloudTrail**: Capture all API calls and activities within your AWS environment to track user activity and API usage.
    - **AWS VPC Flow Logs**: Monitor network traffic flow to and from AWS VPCs to detect anomalous traffic patterns or unauthorized network access attempts.
    - **Security Group Logs**: Analyze changes to security groups to identify unauthorized rule modifications that could expose vulnerable ports or services.
    - **Windows Event Logs**: Collect logs related to system, security, and application events on Windows machines. This includes tracking user logons, system errors, and service start or stop activities.
    - **Linux syslogs**: Monitor system logs for security events, such as authentication failures, sudo access, and system errors, providing insights into potential security incidents on Linux systems.
    - **Splunk Add-ons and Apps**: Utilize the "Splunk Add-on for Amazon Web Services" to streamline the ingestion and parsing of AWS log data, ensuring comprehensive visibility into your cloud infrastructure.

2. Comprehensive Monitoring and Analysis

- **Intrusion Detection/Prevention System Logs**:
    - Integrate logs from IDS/IPS tools like Snort to detect patterns and signatures indicative of network intrusions, exploits, and malicious traffic attempting to breach your network defenses.
- **Authentication Logs**:
    - Monitor for repeated failed login attempts and unusual login patterns (e.g., logins at odd hours or from unexpected locations) to identify brute force attacks or compromised credentials.

- **Network Traffic Data**:
    - Analyze network flow data to identify unusual activity patterns, such as unexpected spikes in traffic, traffic to known bad ports, or traffic originating from or destined to suspicious or geographically unusual locations.
- **Endpoint Detection and Response (EDR) Logs**:
    - Collect and analyze logs from EDR tools to identify signs of malware, ransomware, or other malicious activities on endpoints, enabling early detection of compromises.
- **Threat Intelligence Feeds**:
    - Integrate real-time threat intelligence feeds to enrich log data with context on known malicious IPs, domains, and file hashes, enhancing the detection of threats and reducing false positives.
- **Command and Control (C2) Communication**:
    - Monitor for network communications that match patterns typical of C2 channels, such as irregular DNS requests, beaconing patterns, and traffic to known C2 servers.
- **File Integrity Monitoring**:
    - Implement monitoring of critical system files and configurations for unauthorized changes, which could indicate system tampering or compromise by attackers.
- **Use of Exploit Tools**:
    - Detect the use of known exploit tools and scripts within your network, indicative of active attack attempts or reconnaissance by attackers.
- **Data Exfiltration Attempts**:
    - Monitor for large or unusual data transfers, especially to external destinations, which may indicate attempts to exfiltrate sensitive data from your network.
- **Lateral Movement**:
    - Detect signs of lateral movement within your network, such as the use of administrative tools in unusual contexts or authentication attempts to multiple systems, suggesting efforts by attackers to expand their foothold.

3. Pre-Exercise Preparations

- **Sensor Review**:
    - Conduct a comprehensive review of all network and host-based sensors to ensure they are properly configured and capable of capturing the necessary data for analysis.
- **Traffic Baseline**:
    - Establish a baseline of normal network and system behavior to facilitate the identification of deviations that may signify an attack or malicious activity.
- **Custom Parsing and Data Normalization**:
    - Develop and test custom parsing rules and data normalization techniques to ensure the consistent formatting of log data, enabling more effective analysis and correlation.
- **Indexing and Retention Policies**:
    - Review and adjust indexing and retention policies in Splunk to manage data volumes efficiently while ensuring that critical log data is retained for sufficient periods to support investigation and compliance needs.
- **Isolation and Containment Mechanisms**:

- Implement mechanisms for the rapid isolation or containment of compromised systems to prevent further spread of an attack, minimizing impact on the broader network.

4. Splunk Environment Configuration Checklist

- **Data Sources**:
  - Ensure comprehensive data ingestion from all identified sources, verifying that Splunk connectors, add-ons, and integrations are correctly configured and operational.
- **Real-time Monitoring and Alerts**:
  - Leverage Splunk's real-time monitoring capabilities to generate immediate alerts on detection of suspicious activities, using well-defined criteria and thresholds to minimize response times.
    - Step 1: Log into Splunk
    - Navigate to your Splunk instance login page in a web browser.
    - Enter your credentials to access the Splunk dashboard.

    - Step 2: Define the Search Criteria
    - Consider what constitutes suspicious activity for your environment. This example focuses on failed logins, process creations involving PowerShell or command prompt indicative of script execution, and certain web server error messages.

    - Step 3: Create a New Search
    - Navigate to the "Search & Reporting" app within Splunk.
    - Enter the following search query to monitor for suspicious activities:
    - **Lua Copy code**

```
(index="main" (host="RISK-ANALYST1" OR host="ACCOUNTING1" OR host="ACCOUNTING2" OR host="CFO-LAPTOP" OR host="ip-10-0-0-175") AND ( (sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND ("Process Create" AND (CommandLine="*powershell.exe*" OR CommandLine="*cmd.exe /c*"))) OR (sourcetype="WinEventLog:Security" AND (EventCode=4625 OR EventCode=4740)) OR  (sourcetype="linux_secure" AND "Failed password" AND NOT user="known_good_user") OR  (sourcetype="apache_error" AND ("client denied by server configuration" OR "File does not exist" OR "script not found or unable to stat")) ))| eval AttackDetected=if(match(_raw, "Process Create|EventCode=4625|EventCode=4740|Failed password|client denied by server configuration|File does not exist|script not found or unable to stat"), "Yes", "No")| table _time, host, AttackDetected, sourcetype, _raw | sort - _time
```

    - Adjust the time range to "Real-time" and execute the search to confirm it provides the expected results.

- Step 4: Save the Search as an Alert
- Click "Save As" > "Alert".
- Provide a meaningful title and description for the alert.

- Step 5: Configure Alert Settings
- Alert Type: Choose "Real-time".
- Trigger Conditions: Define the conditions, such as if the event count exceeds a threshold.
- Throttle: Set to prevent too many alerts in a short period.

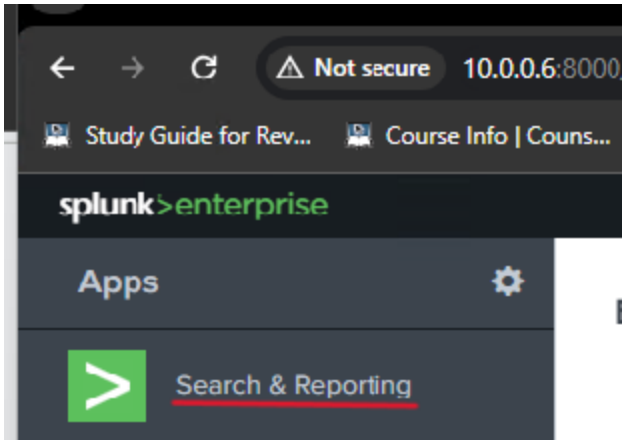
- Step 6: Set Up Alert Actions
- Send Email: Configure email notifications with details about the triggered alert.
- Add to Triggered Alerts: Enable logging for review.
- Run a Script: If you have an automated response script, specify it here.

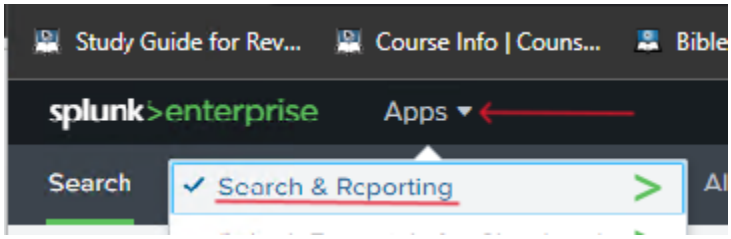
- Step 7: Review and Save the Alert
- Double-check your settings and click "Save" to activate the alert.

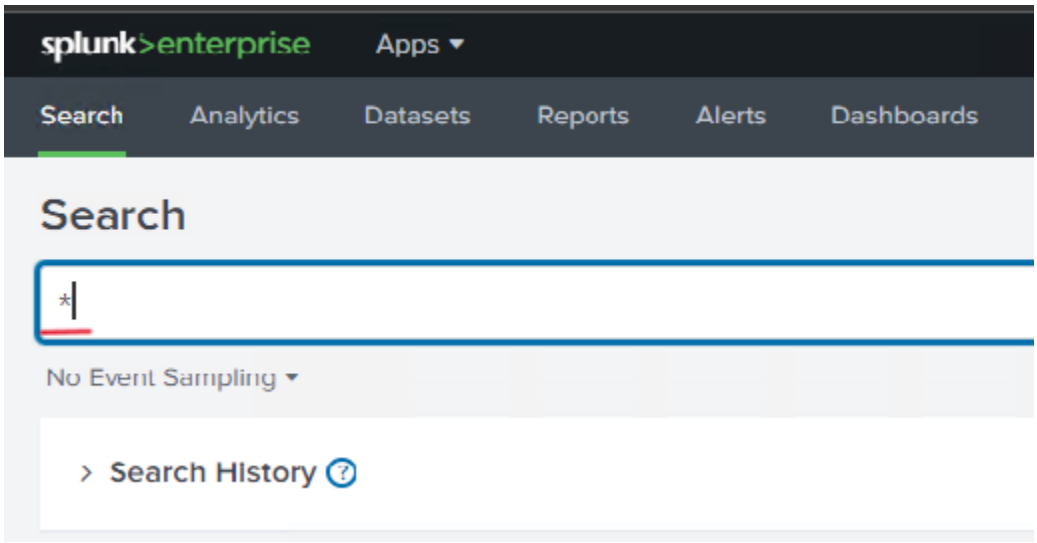
- Step 8: Monitor Alerts and Respond
- Regularly review the "Triggered Alerts" section and your emails for alerts.
- Investigate and respond to alerts as necessary to address potential security incidents.
- This setup allows you to proactively monitor and respond to signs of compromise in real-time, crucial for maintaining the security posture of your environment.

- **Dashboards**:
  - Design and deploy dashboards that provide a real-time overview of the security posture, showcasing key metrics, and indicators of compromise to facilitate quick situational awareness and decision-making.

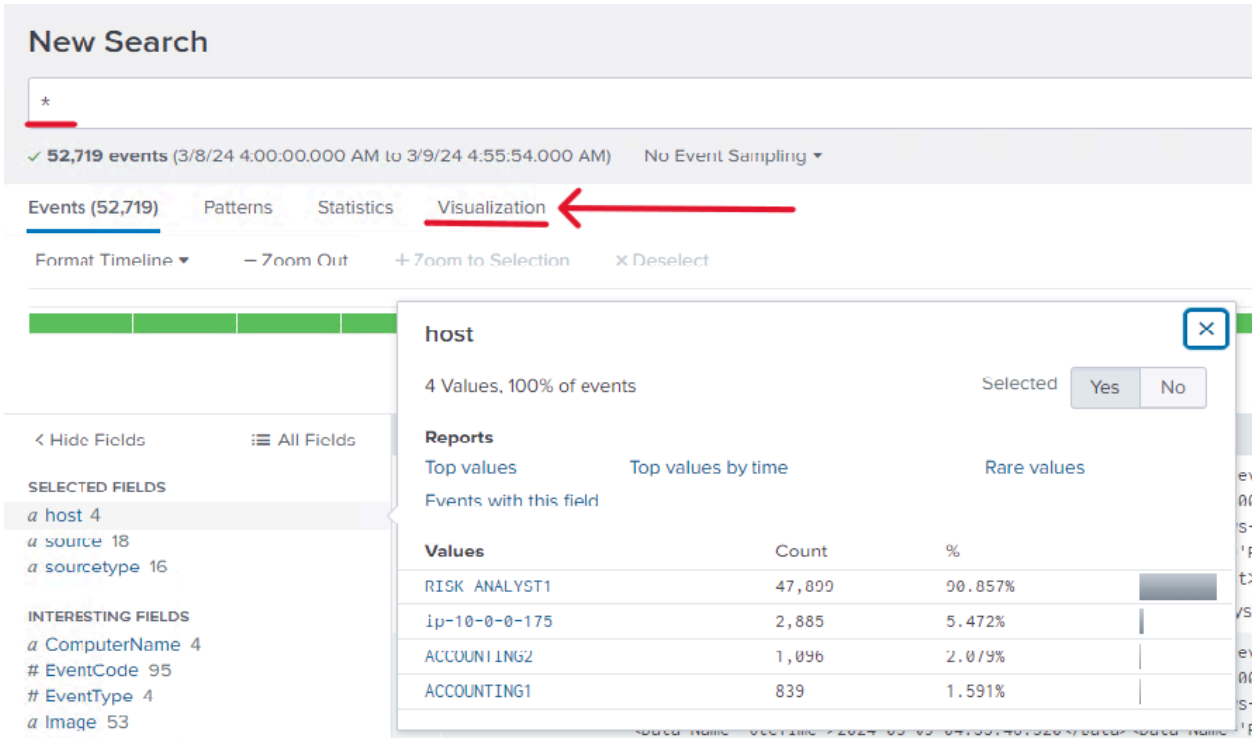
Setting up Network Monitoring and Alerts:

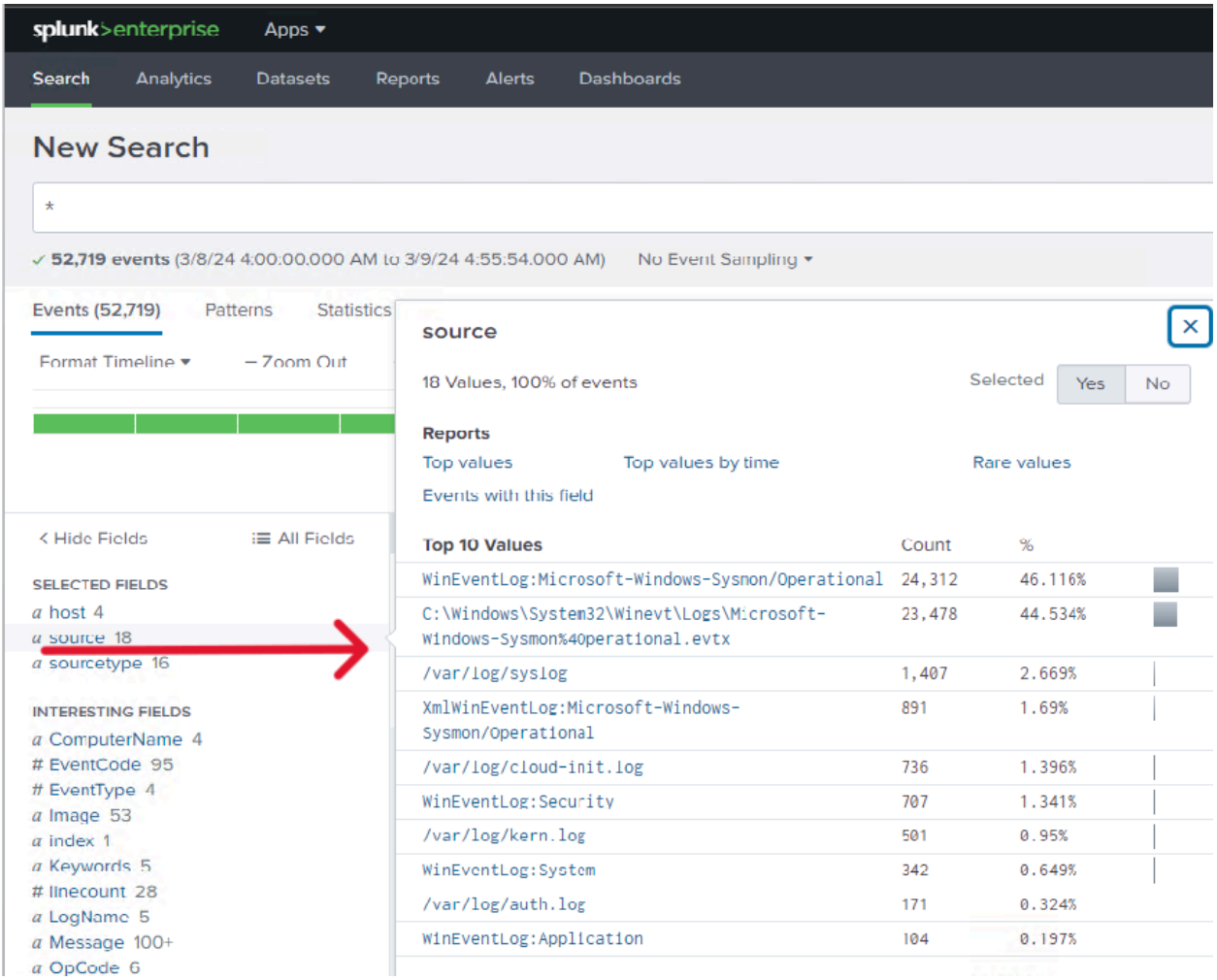


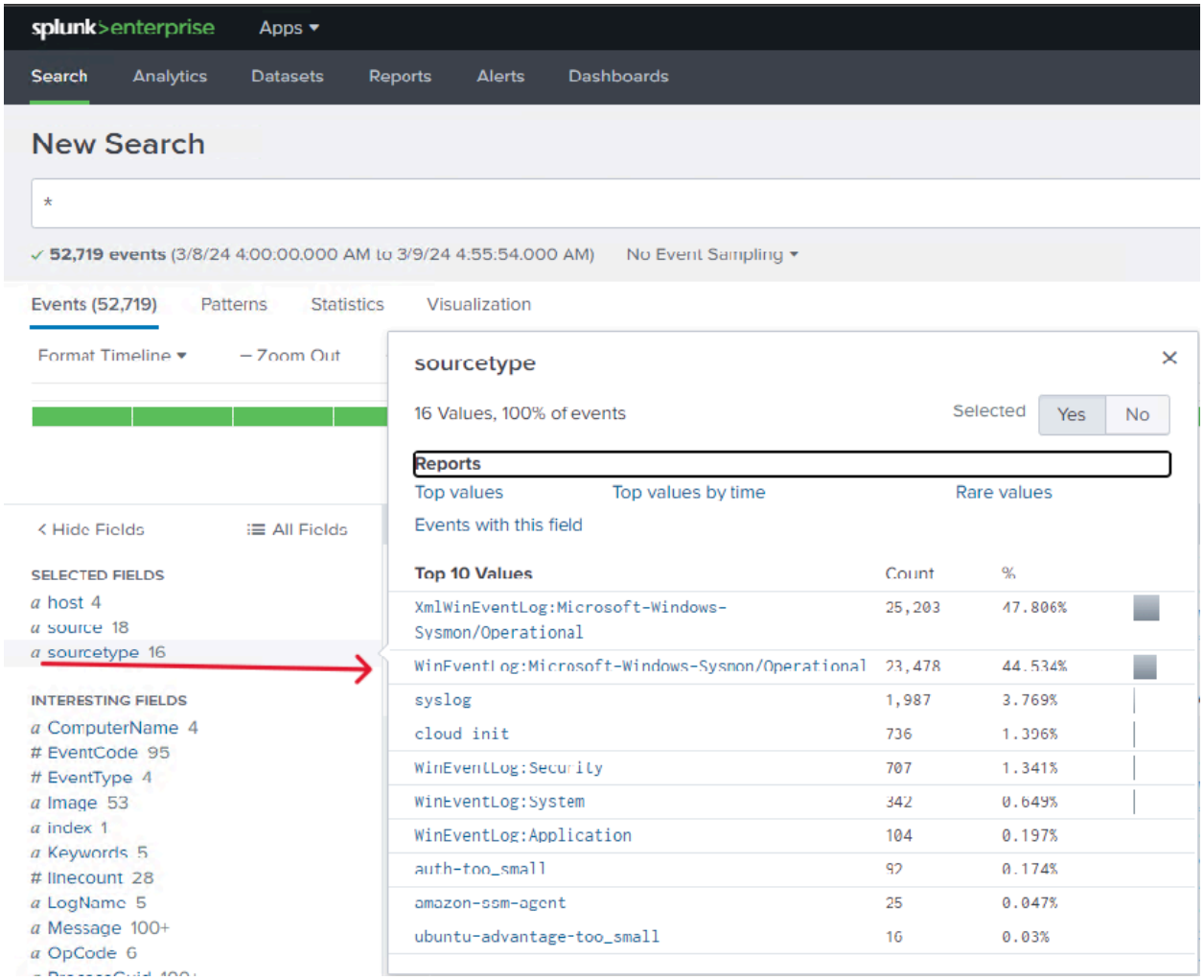


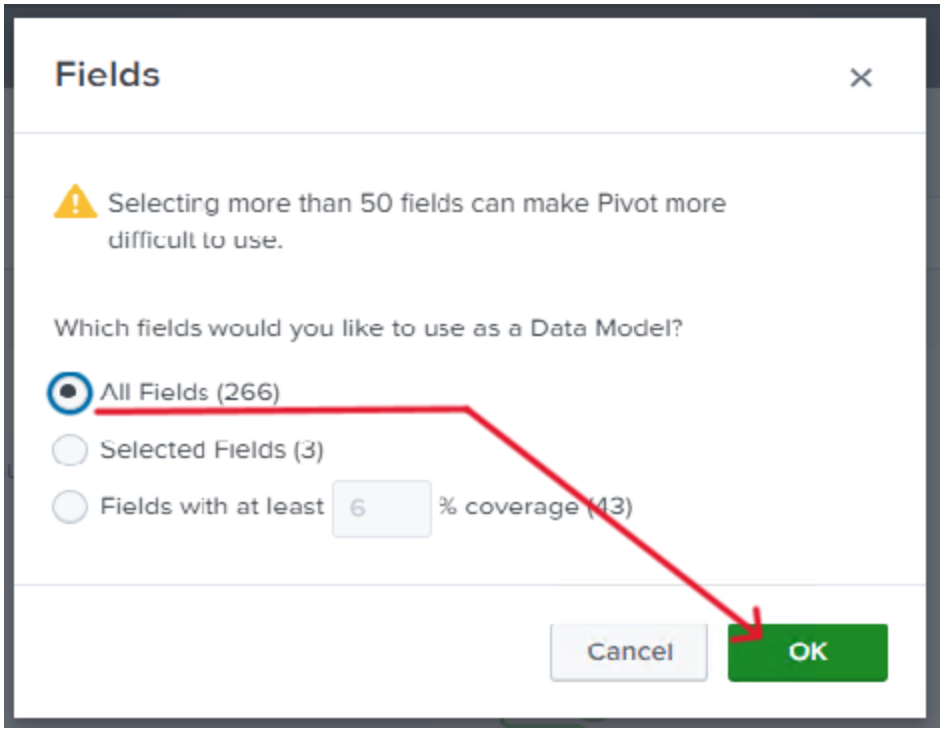


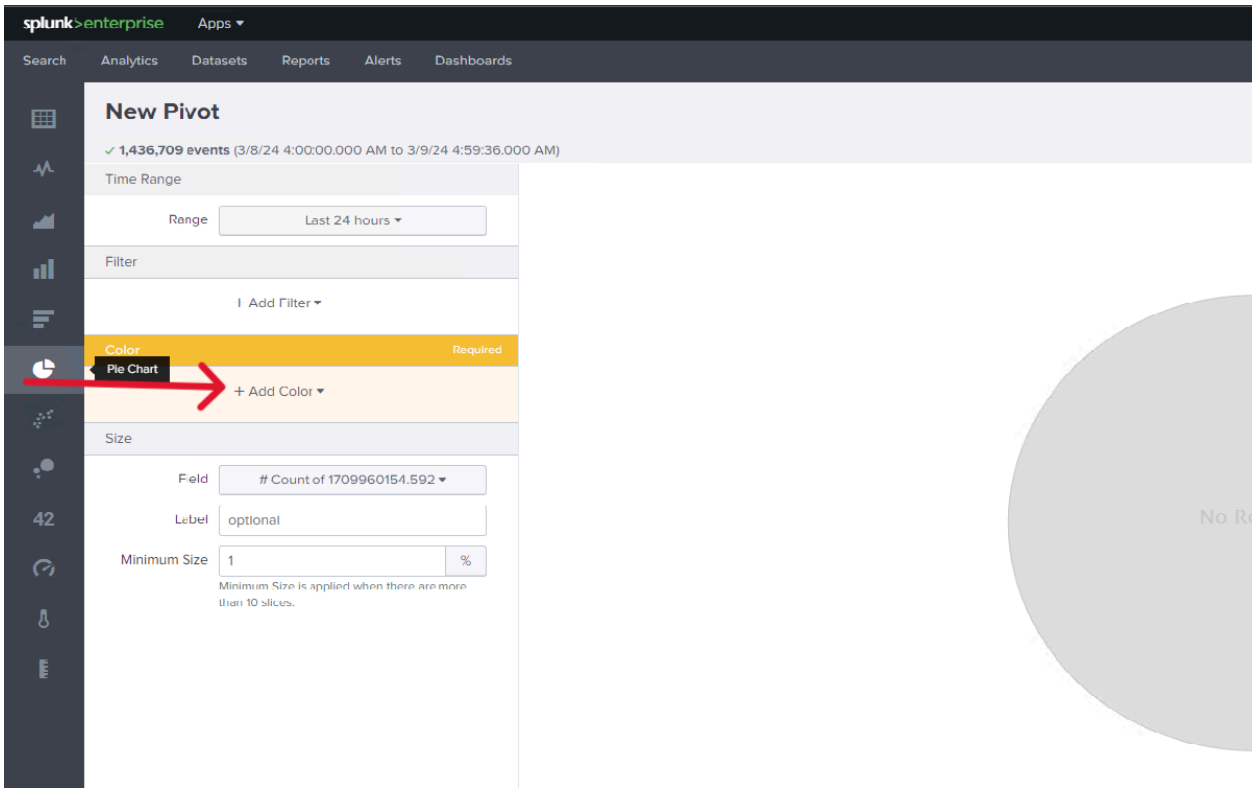
Just put the asterisk in the search bar and hit enter.

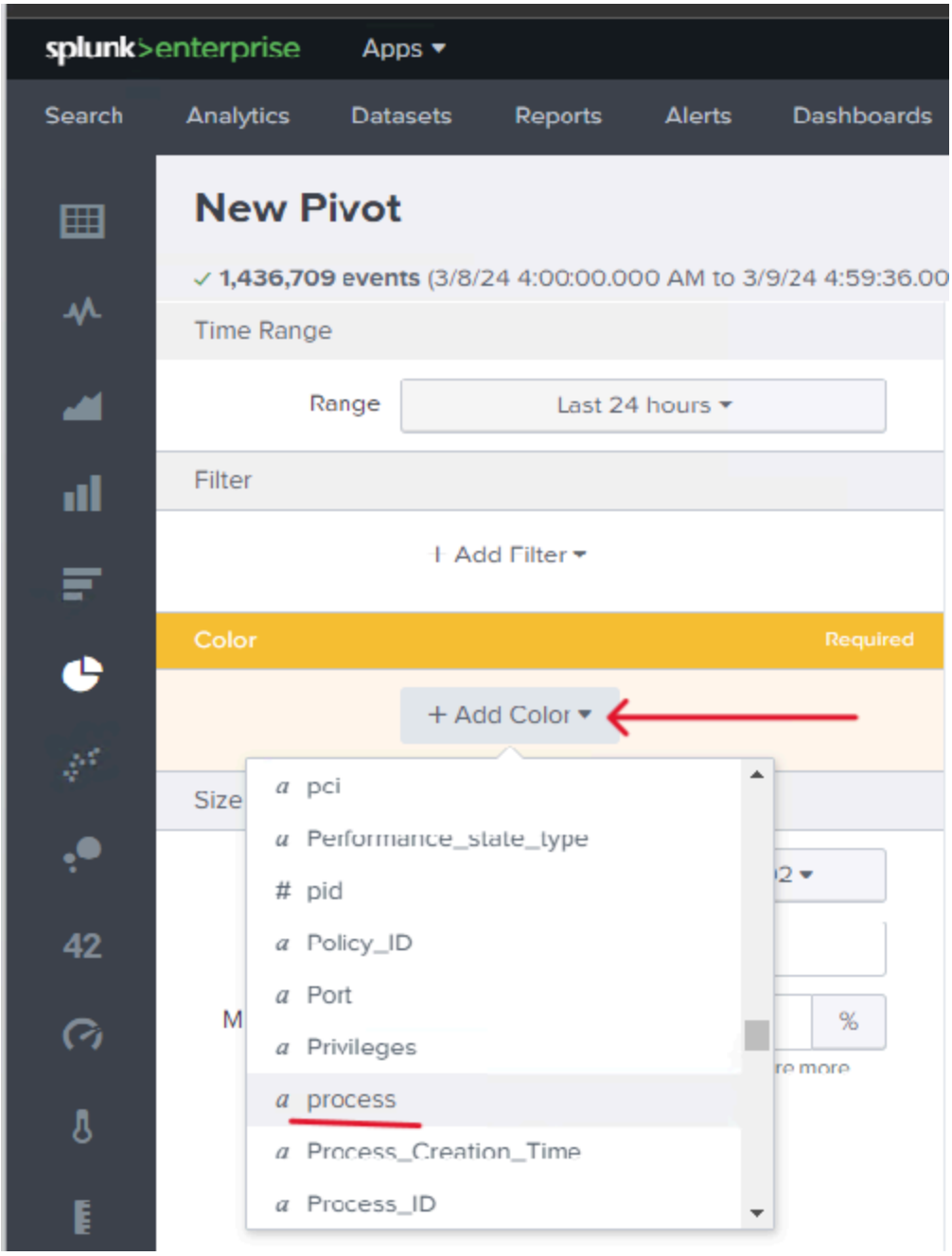

New Search
*
✓ 52,719 events (3/8/24 4:00:00.000 AM to 3/9/24 4:55:54.000 AM)
No Event Sampling
Events (52,719)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
host
4 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
RISK ANALYST1
47,899
90.857%
ip-10-0-0-175
2,885
5.472%
ACCOUNTING2
1,096
2.079%
ACCOUNTING1
839
1.591%
< Hide Fields
All Fields
SELECTED FIELDS
a host 4
a source 18
a sourcetype 16
INTERESTING FIELDS
a ComputerName 4
EventCode 95
EventType 4
a Image 53

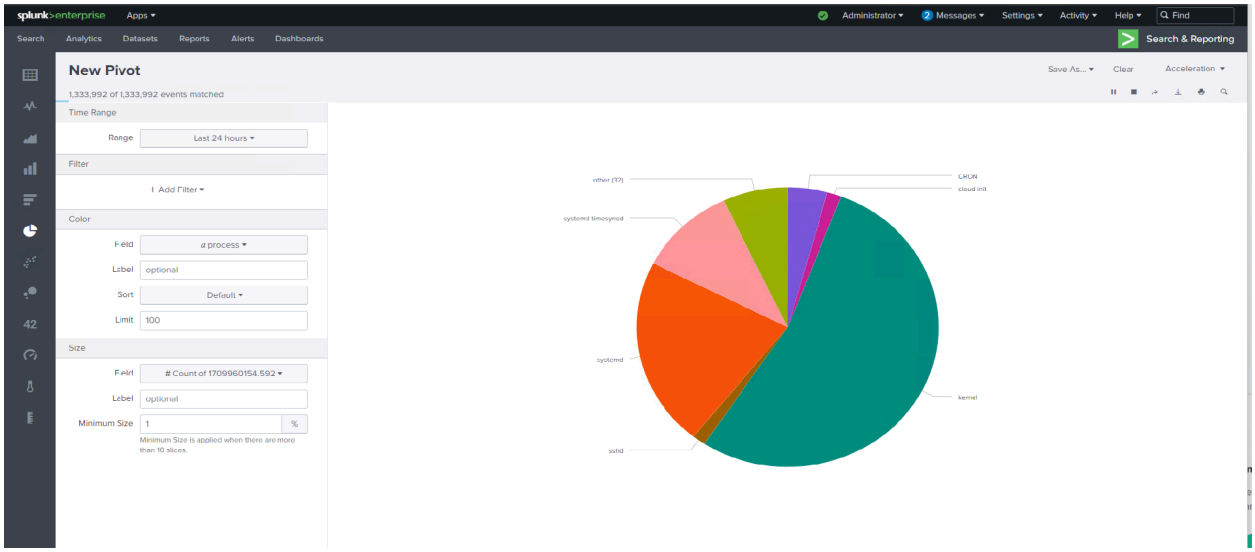

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
*
52,719 events (3/8/24 4:00:00.000 AM to 3/9/24 4:55:54.000 AM)
No Event Sampling
Events (52,719)
Patterns
Statistics
Format Timeline
– Zoom Out
Hide Fields
All Fields
SELECTED FIELDS
a host 4
a source 18
a sourcetype 16
INTERESTING FIELDS
a ComputerName 4
EventCode 95
EventType 4
a Image 53
a index 1
a Keywords 5
linecount 28
a LogName 5
a Message 100+
a OpCode 6
source
18 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
WinEventLog:Microsoft-Windows-Sysmon/Operational 24,312 46.116%
C:\Windows\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx 23,478 44.534%
/var/log/syslog 1,407 2.669%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational 891 1.69%
/var/log/cloud-init.log 736 1.396%
WinEventLog:Security 707 1.341%
/var/log/kern.log 501 0.95%
WinEventLog:System 342 0.649%
/var/log/auth.log 171 0.324%
WinEventLog:Application 104 0.197%

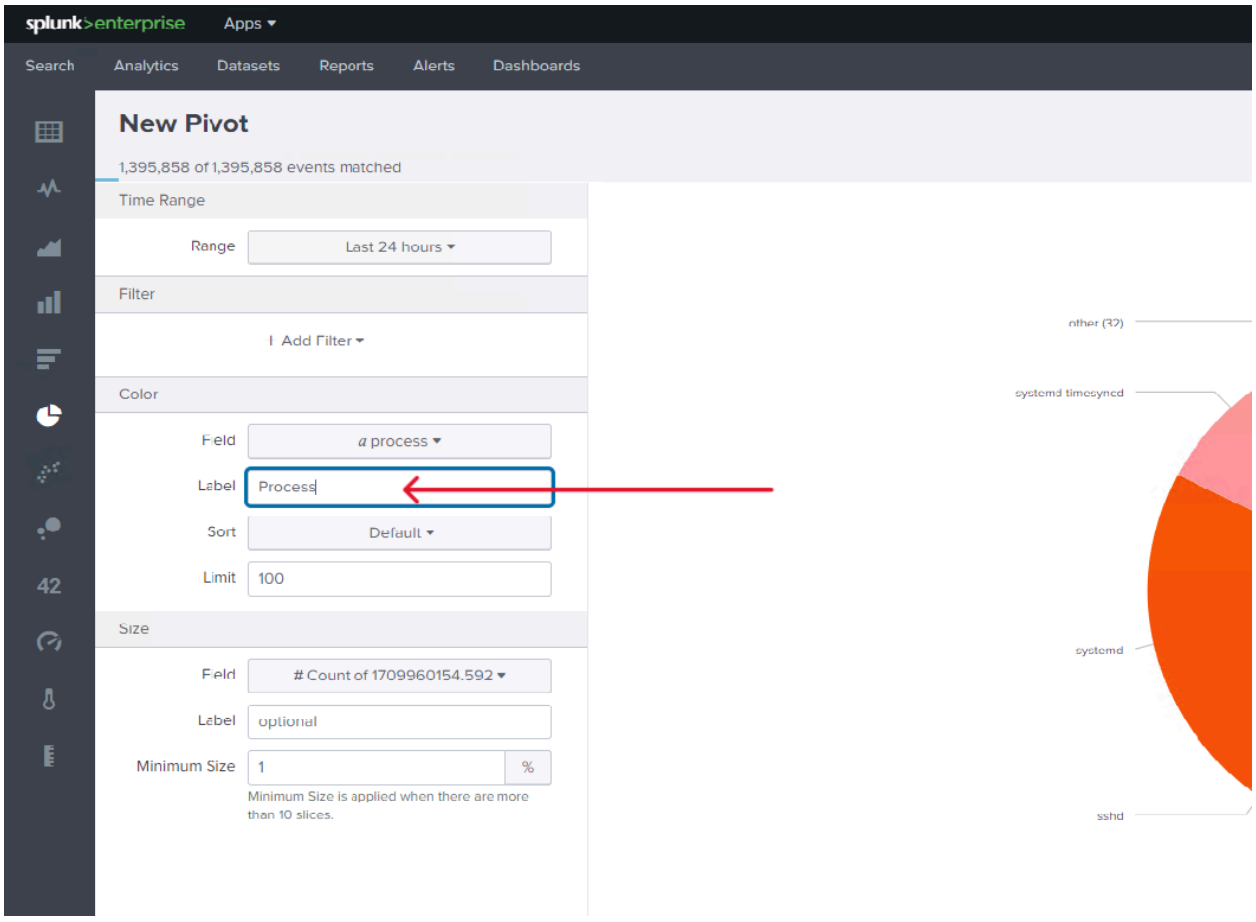

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
*
52,719 events (3/8/24 4:00:00.000 AM to 3/9/24 4:55:54.000 AM)
No Event Sampling
Events (52,719)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Hide Fields
All Fields
SELECTED FIELDS
a host 4
a source 18
a sourcetype 16
INTERESTING FIELDS
a ComputerName 4
EventCode 95
EventType 4
a Image 53
a index 1
a Keywords 5
linecount 28
a LogName 5
a Message 100+
a OpCode 6
sourcetype
16 Values, 100% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
25,203
47.806%
WinEventLog:Microsoft-Windows-Sysmon/Operational
23,478
44.534%
syslog
1,987
3.769%
cloud_init
736
1.396%
WinEventLog:Security
707
1.341%
WinEventLog:System
342
0.649%
WinEventLog:Application
104
0.197%
auth-too_small
92
0.174%
amazon-ssm-agent
25
0.047%
ubuntu-advantage-too_small
16
0.03%

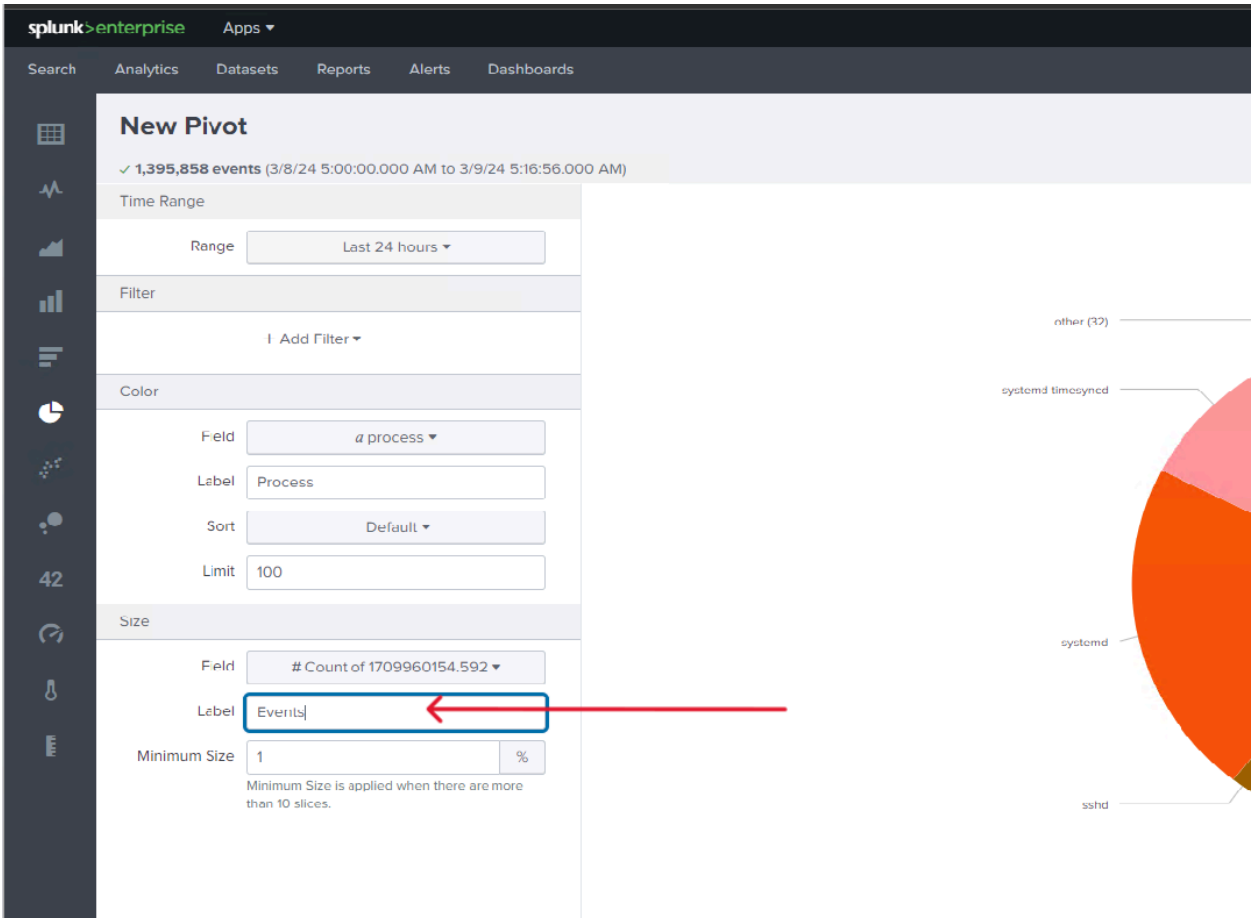

Fields
Selecting more than 50 fields can make Pivot more difficult to use.
Which fields would you like to use as a Data Model?
All Fields (266)
Selected Fields (3)
Fields with at least 6 % coverage (43)
Cancel
OK


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,436,709 events (3/8/24 4:00:00.000 AM to 3/9/24 4:59:36.000 AM)
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Required
Pie Chart
+ Add Color
Size
Field
Count of 1709960154.592
Label
optional
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.

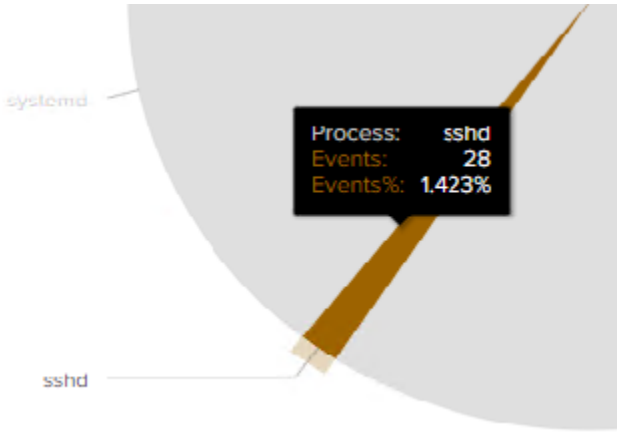

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,436,709 events (3/8/24 4:00:00.000 AM to 3/9/24 4:59:36.00
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Required
+ Add Color
Size
pci
Performance_state_type
pid
Policy_ID
Port
Privileges
process
Process_Creation_Time
Process_ID

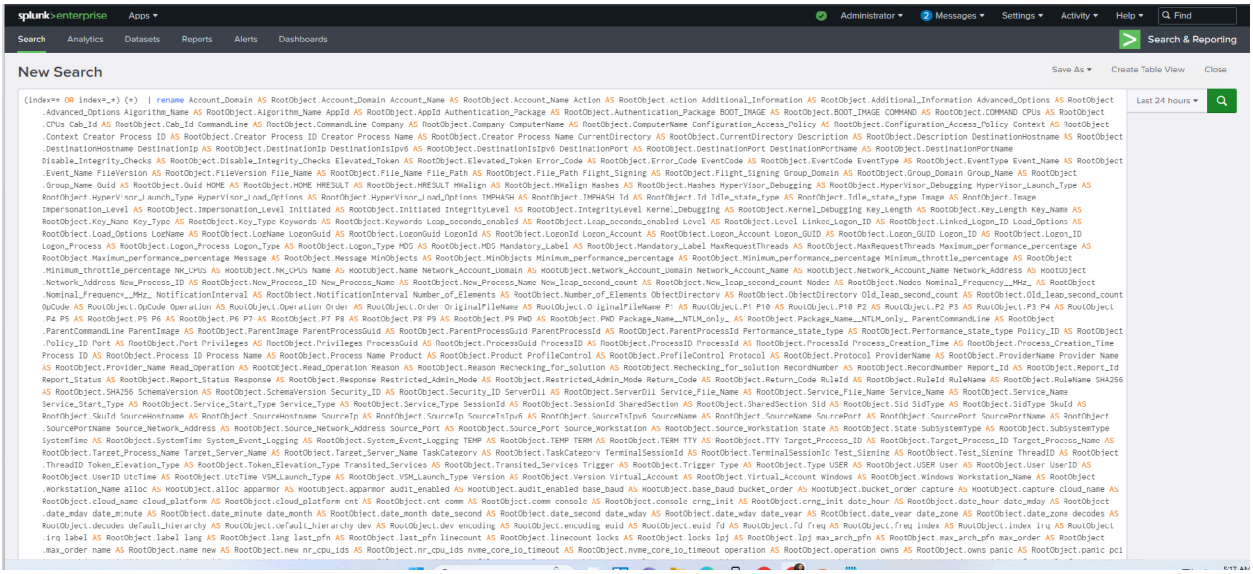

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
1,333,992 of 1,333,992 events matched
Save As...
Clear
Acceleration
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Field
a process
Label
optional
Sort
Default
Limit
100
Size
Field
Count of 1709960154.592
Label
optional
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.
other (32)
CRON
cloud-init
systemd-timesyncd
systemd
kernel
sshd

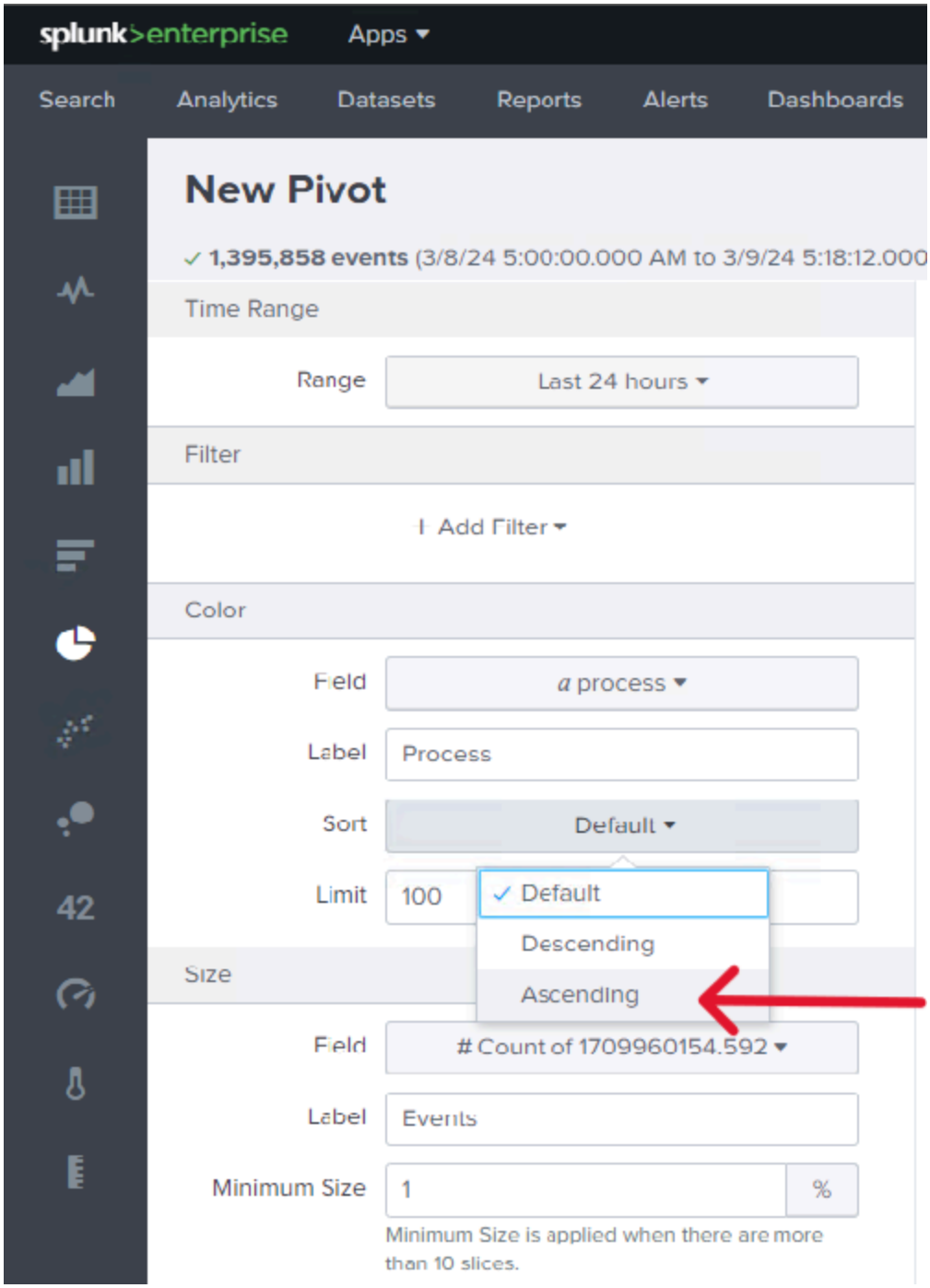

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,395,858 of 1,395,858 events matched
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Field
a process
Label
Process
Sort
Default
Limit
100
Size
Field
Count of 1709960154.592
Label
optional
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.
other (32)
systemd-timesyncd
systemd
sshd

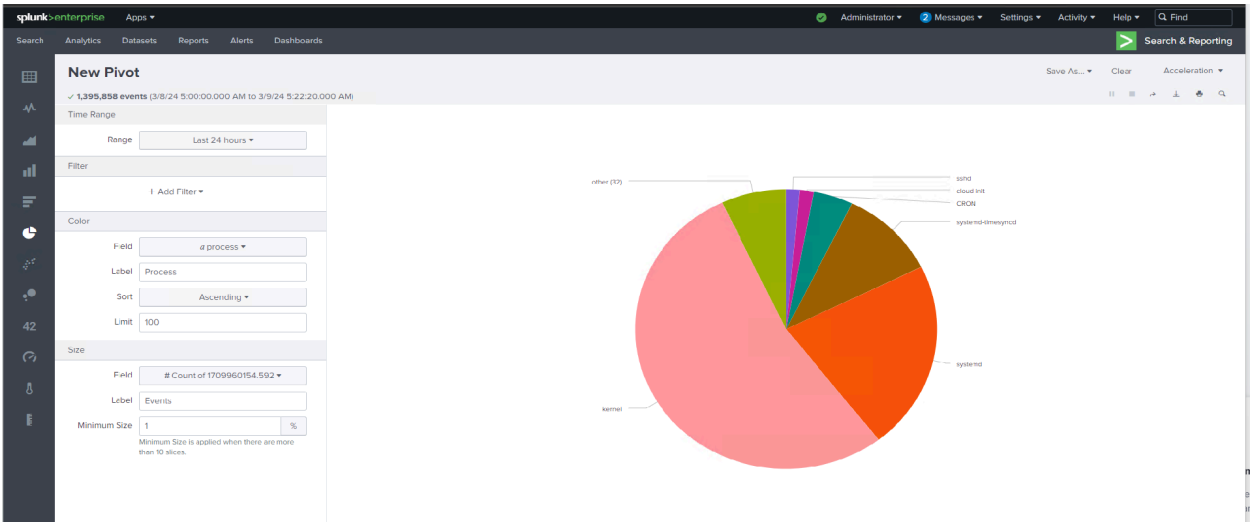

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,395,858 events (3/8/24 5:00:00.000 AM to 3/9/24 5:16:56.000 AM)
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Field
a process
Label
Process
Sort
Default
Limit
100
Size
Field
Count of 1709960154.592
Label
Events
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.

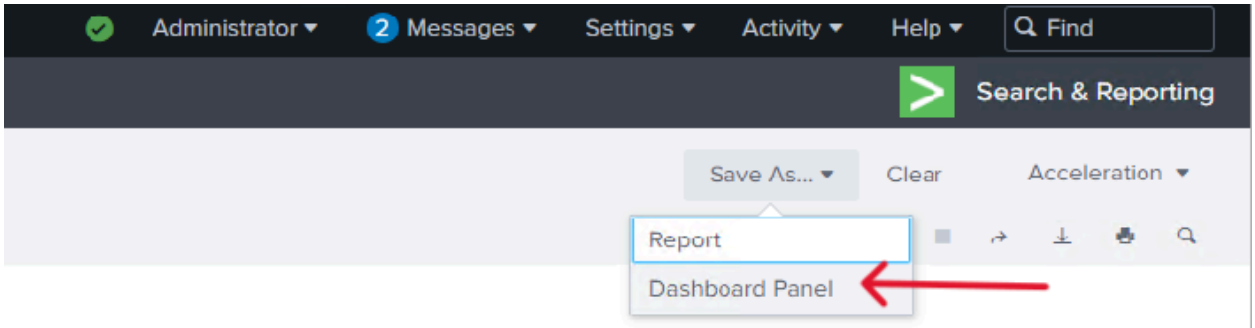
other (32)
systemd timesynced
systemd
sshd

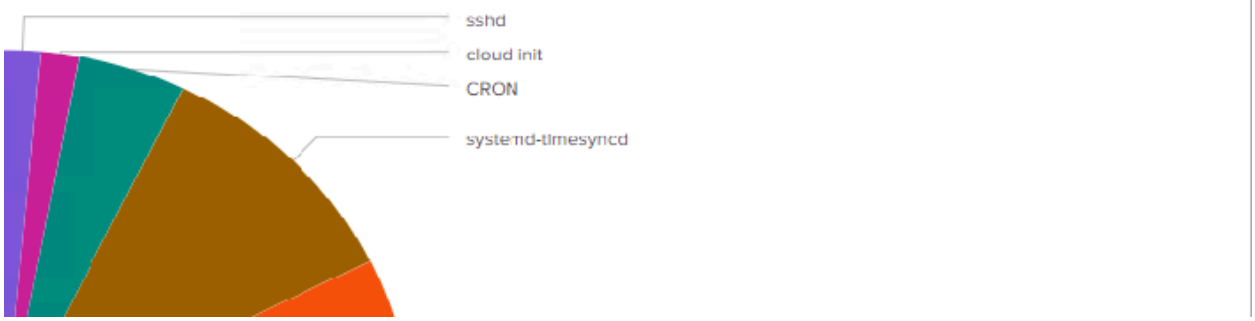

systemd
Process: sshd
Events: 28
Events%: 1.423%
sshd

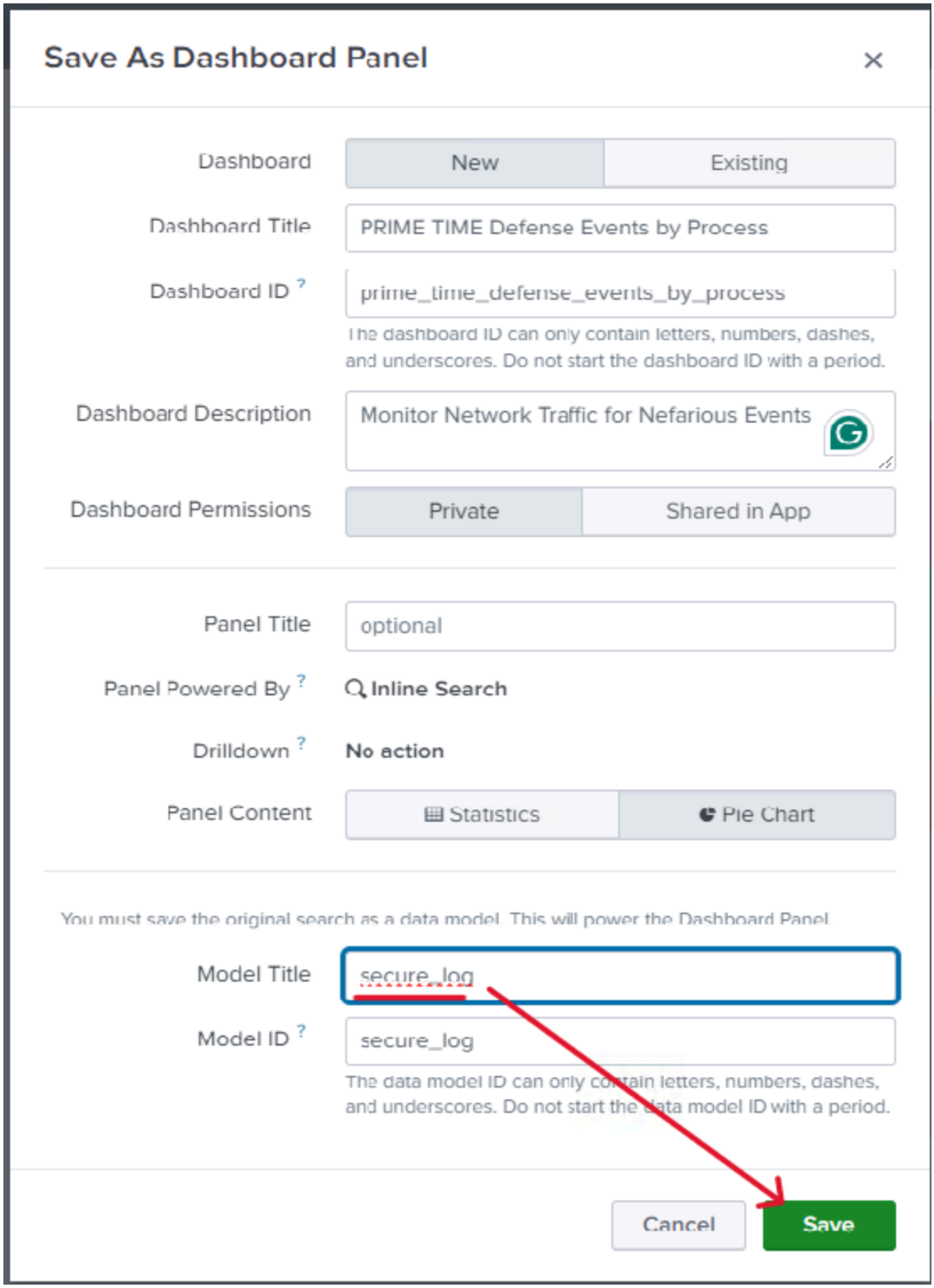

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
Last 24 hours

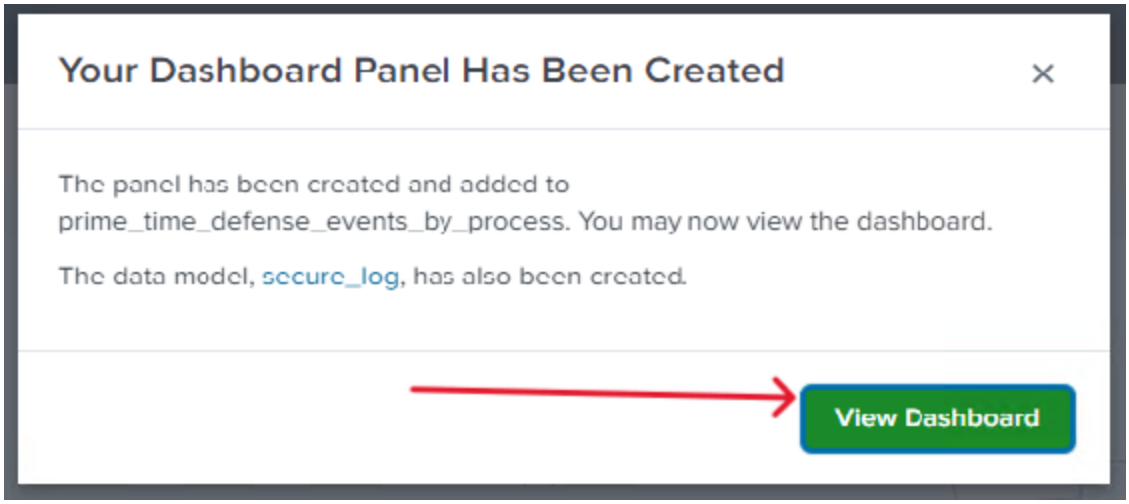

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,395,858 events (3/8/24 5:00:00.000 AM to 3/9/24 5:18:12.000
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Field
a process
Label
Process
Sort
Default
Limit
100
Default
Descending
Ascending
Size
Field
Count of 1709960154.592
Label
Events
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.

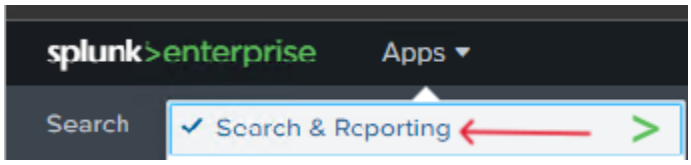

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
Save As...
Clear
Acceleration
1,395,858 events (3/8/24 5:00:00.000 AM to 3/9/24 5:22:20.000 AM)
Time Range
Range
Last 24 hours
Filter
Add Filter
Color
Field
a process
Label
Process
Sort
Ascending
Limit
100
Size
Field
Count of 1709960154.592
Label
Events
Minimum Size
1
%
Minimum Size is applied when there are more than 10 slices.
other (17)
sshd
cloud init
CRON
systemd-timesyncd
systemd
kernel

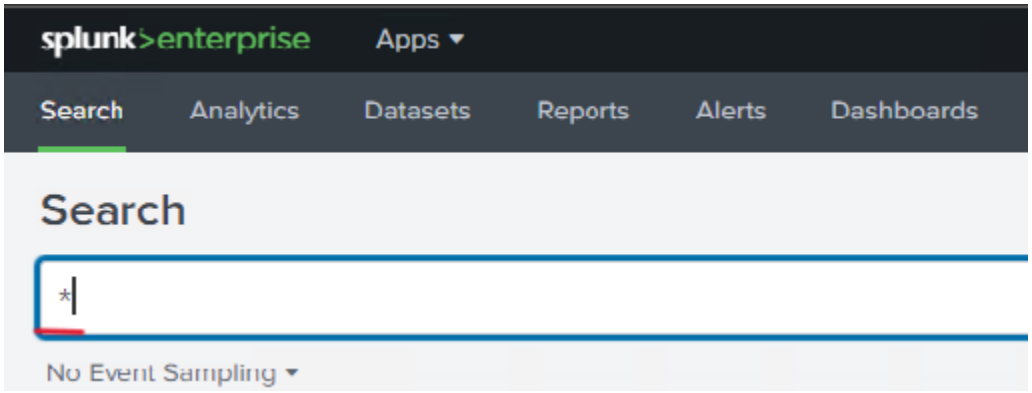

Administrator
2 Messages
Settings
Activity
Help
Find
Search & Reporting
Save As...
Clear
Acceleration
Report
Dashboard Panel

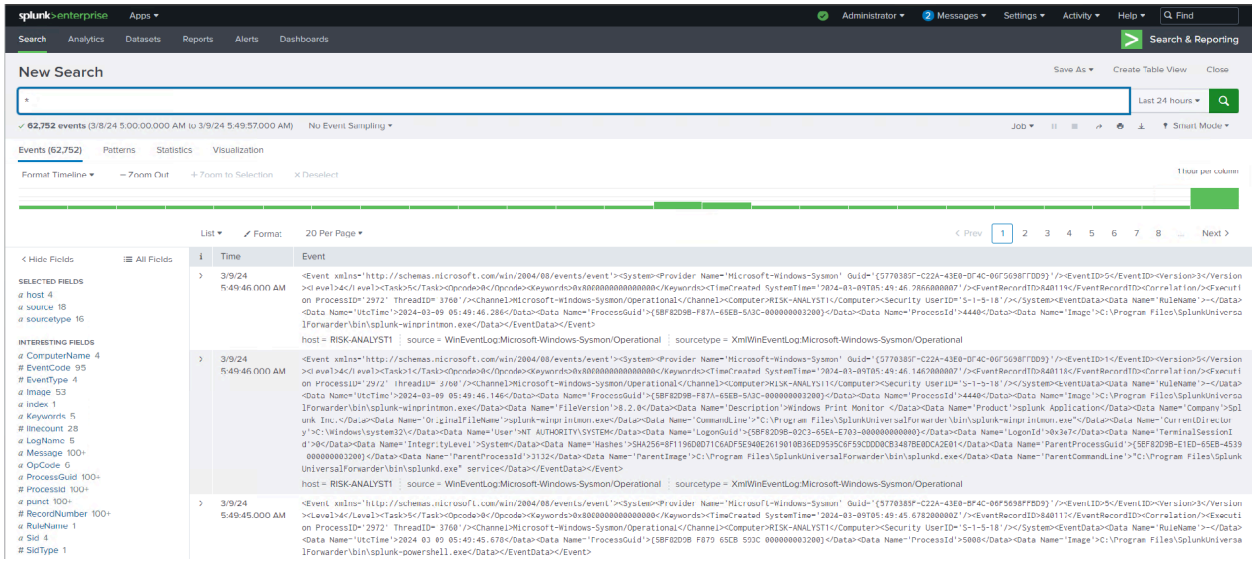

sshd
cloud init
CRON
systemd-timesyncd

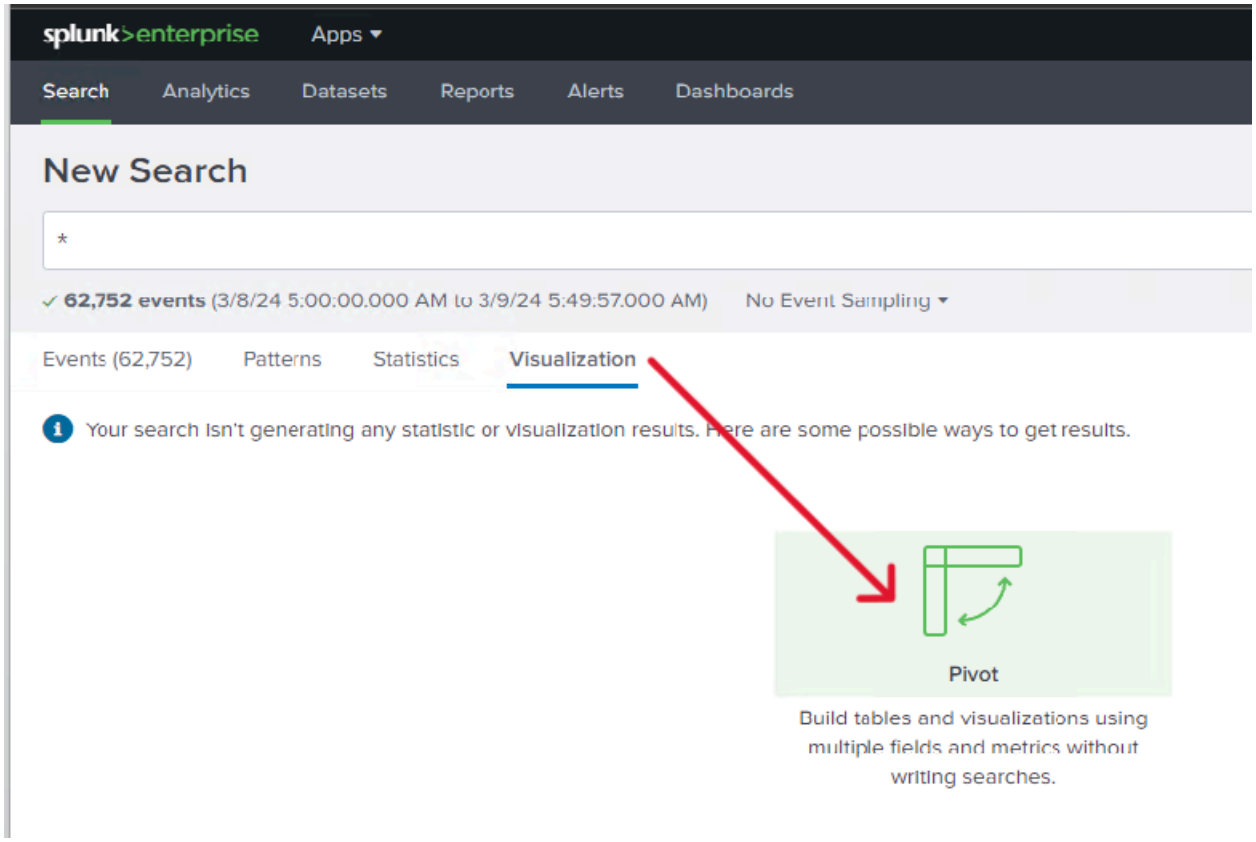

Save As Dashboard Panel
Dashboard
New
Existing
Dashboard Title
PRIME TIME Defense Events by Process
Dashboard ID
prime_time_defense_events_by_process
The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.
Dashboard Description
Monitor Network Traffic for Nefarious Events
Dashboard Permissions
Private
Shared in App
Panel Title
optional
Panel Powered By
Inline Search
Drilldown
No action
Panel Content
Statistics
Pie Chart
You must save the original search as a data model. This will power the Dashboard Panel.
Model Title
secure_log
Model ID
secure_log
The data model ID can only contain letters, numbers, dashes, and underscores. Do not start the data model ID with a period.
Cancel
Save

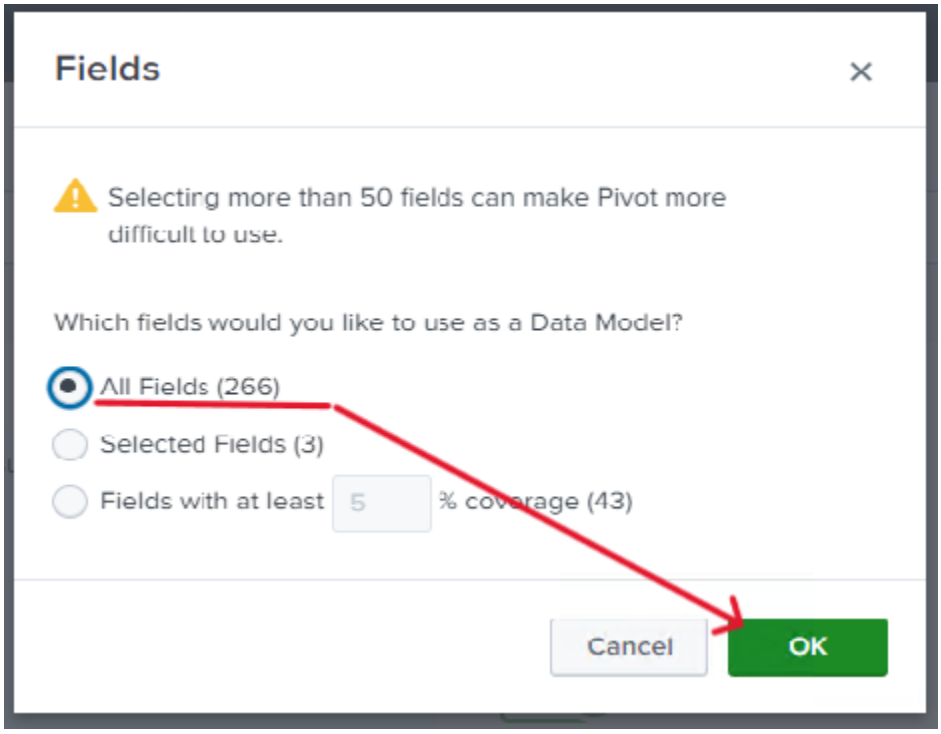

Your Dashboard Panel Has Been Created
The panel has been created and added to prime_time_defense_events_by_process. You may now view the dashboard.
The data model, secure_log, has also been created.
View Dashboard

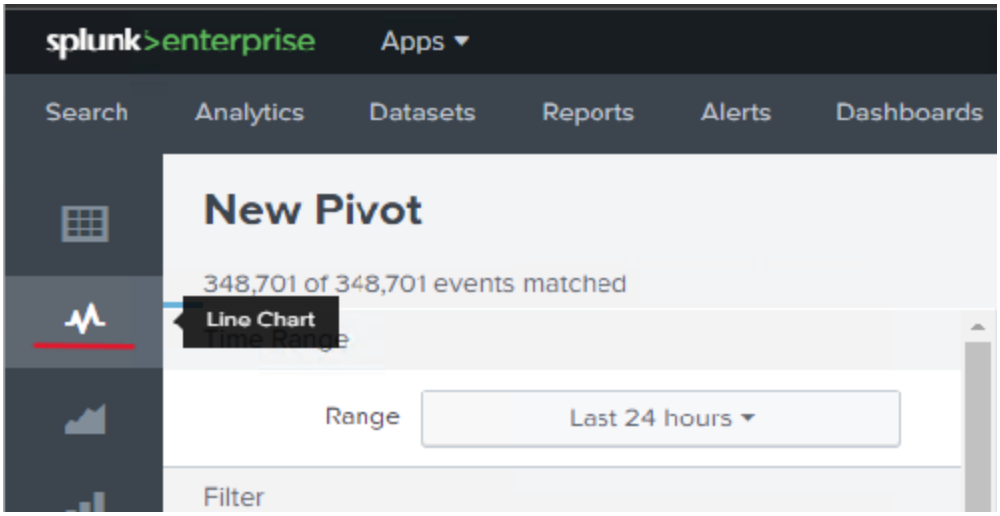

splunk>enterprise
Apps
Search
Search & Reporting

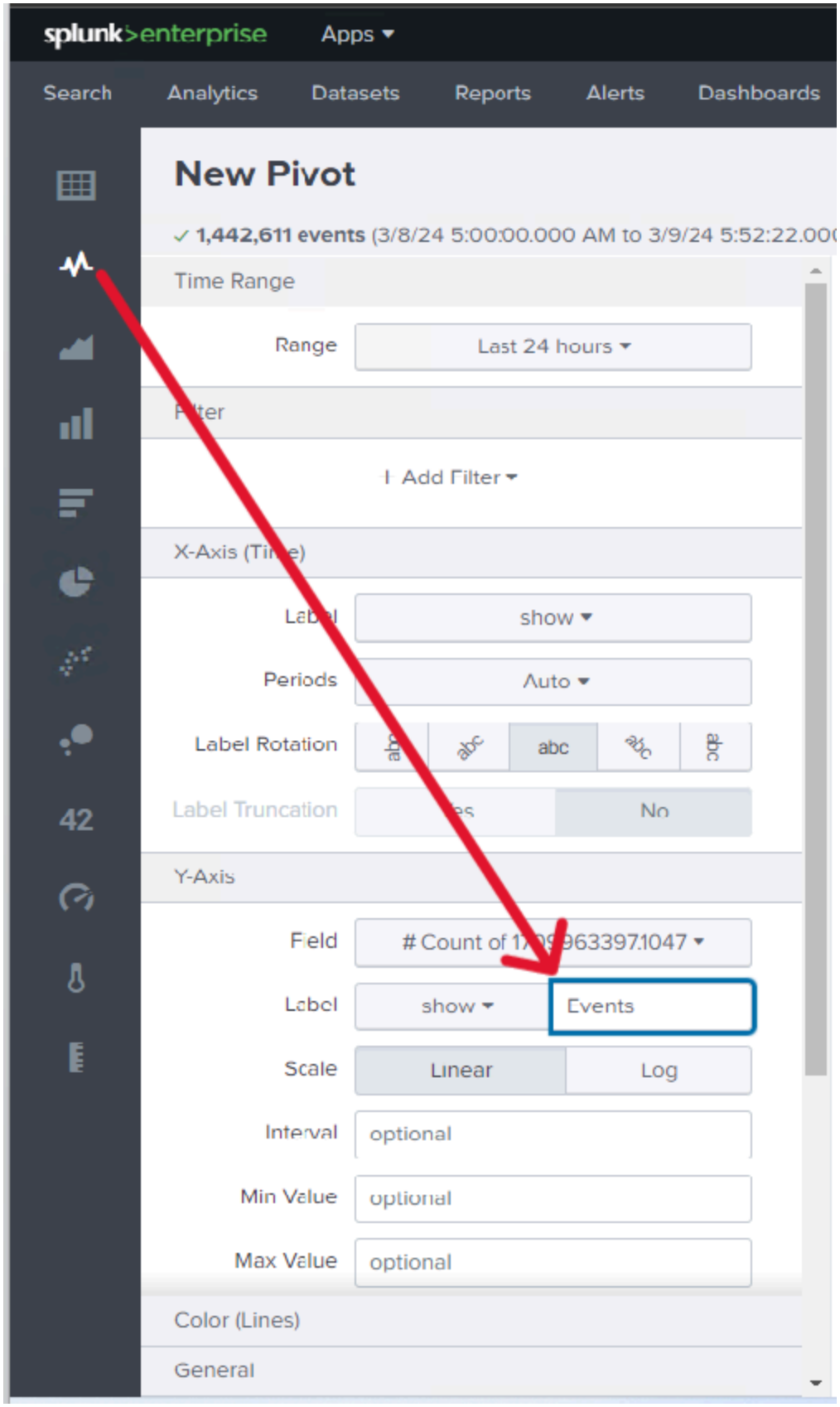

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search
*
No Event Sampling

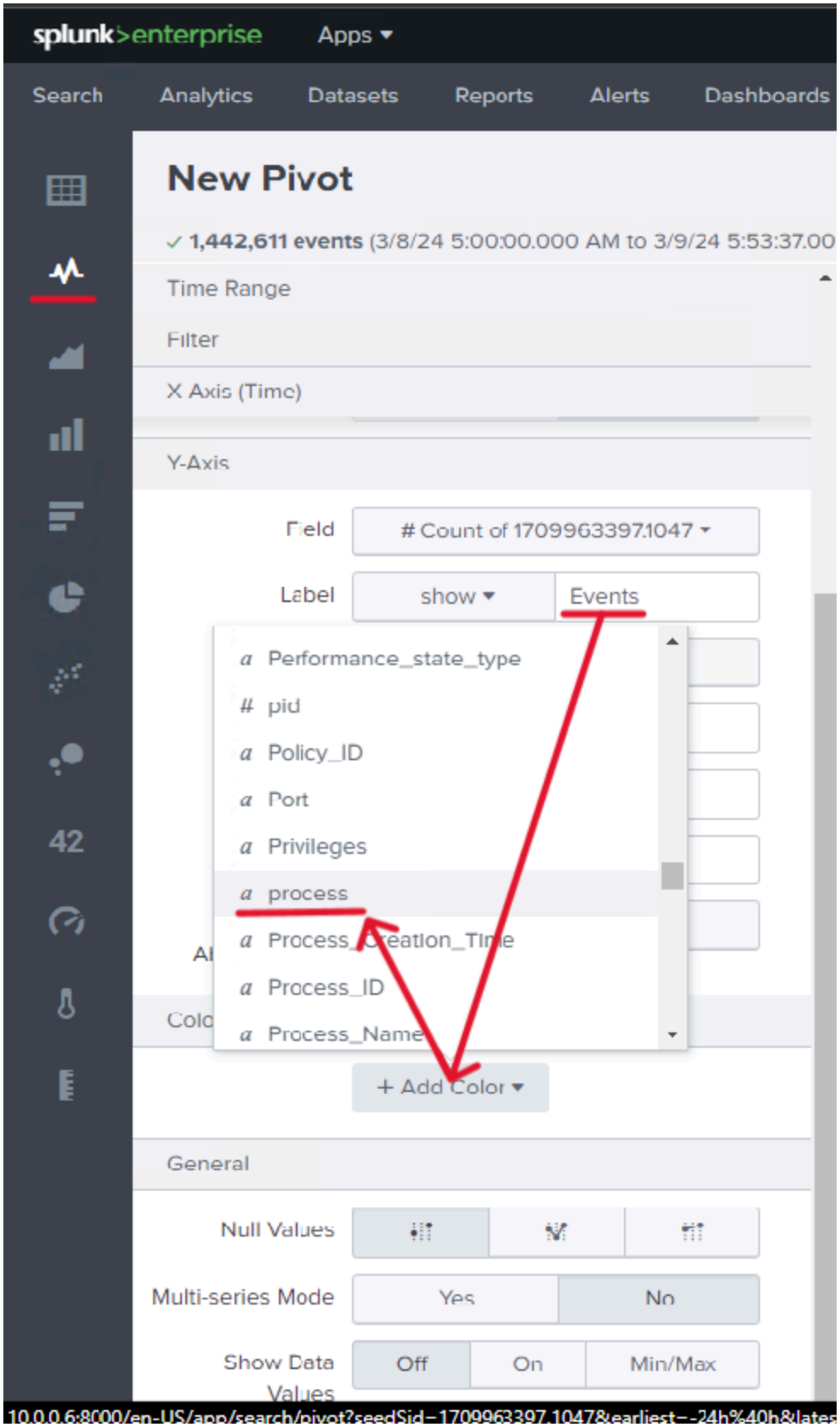

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
Last 24 hours
62,752 events (3/8/24 5:00:00.000 AM to 3/9/24 5:49:57.000 AM)
No Event Sampling
Job
Smart Mode
Events (62,752)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Prev
Next
Hide Fields
All Fields
SELECTED FIELDS
host 4
source 18
sourcetype 16
INTERESTING FIELDS
ComputerName 4
EventCode 95
EventType 4
Image 53
index 1
Keywords 5
linecount 28
LogName 5
Message 100+
OpCode 6
ProcessGuid 100+
ProcessId 100+
punct 100+
RecordNumber 100+
RuleName 1
Sid 4
SidType 1
Time
Event
3/9/24 5:49:46.000 AM
3/9/24 5:49:46.000 AM
3/9/24 5:49:45.000 AM

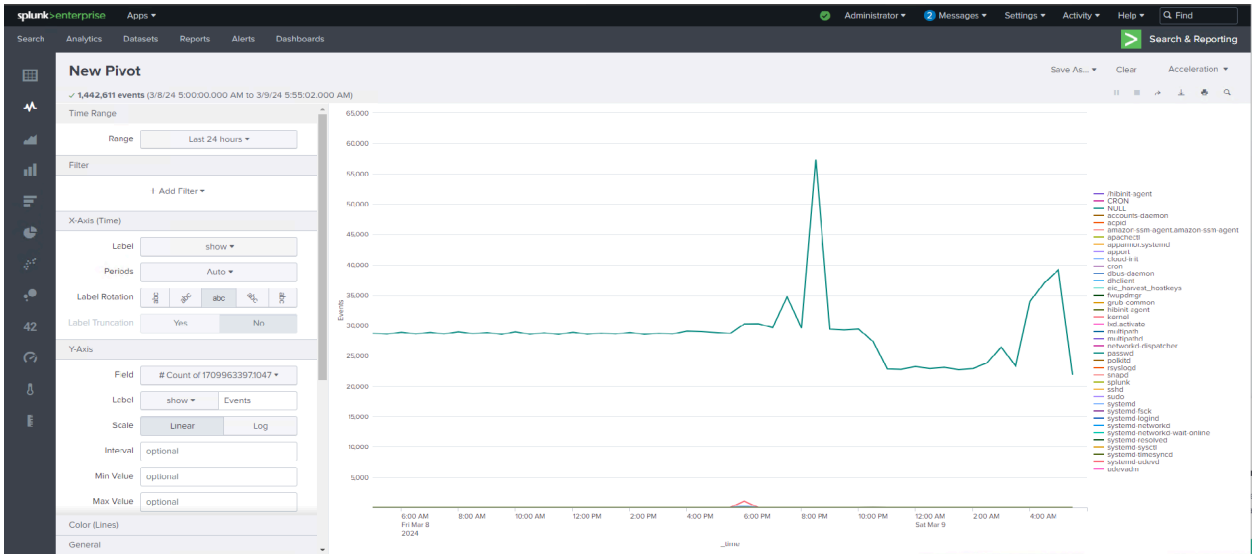

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
*
62,752 events (3/8/24 5:00:00.000 AM to 3/9/24 5:49:57.000 AM)
No Event Sampling
Events (62,752)
Patterns
Statistics
Visualization
Your search isn't generating any statistic or visualization results. Here are some possible ways to get results.
Pivot
Build tables and visualizations using multiple fields and metrics without writing searches.

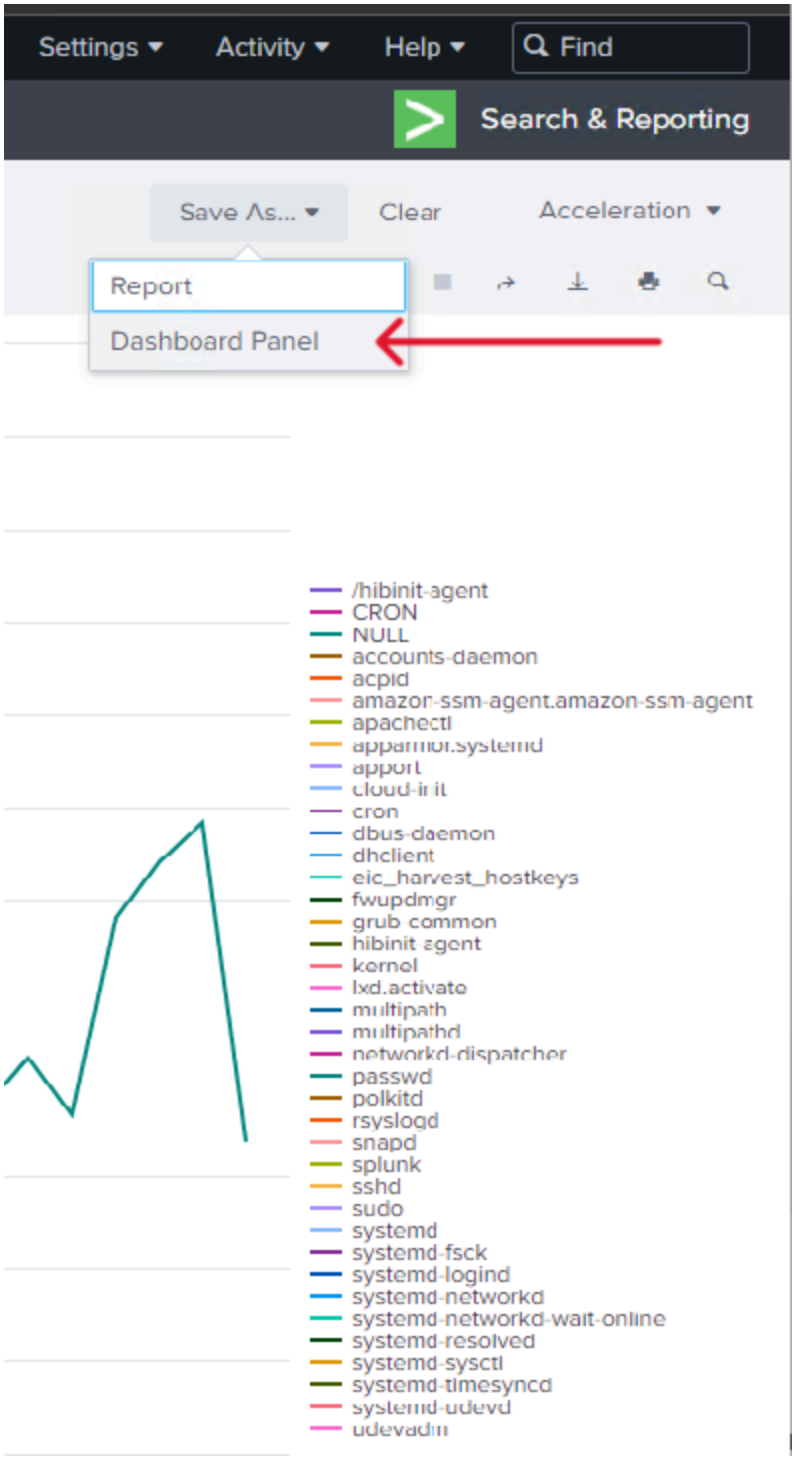

Fields
Selecting more than 50 fields can make Pivot more difficult to use.
Which fields would you like to use as a Data Model?
All Fields (266)
Selected Fields (3)
Fields with at least 5 % coverage (43)
Cancel
OK

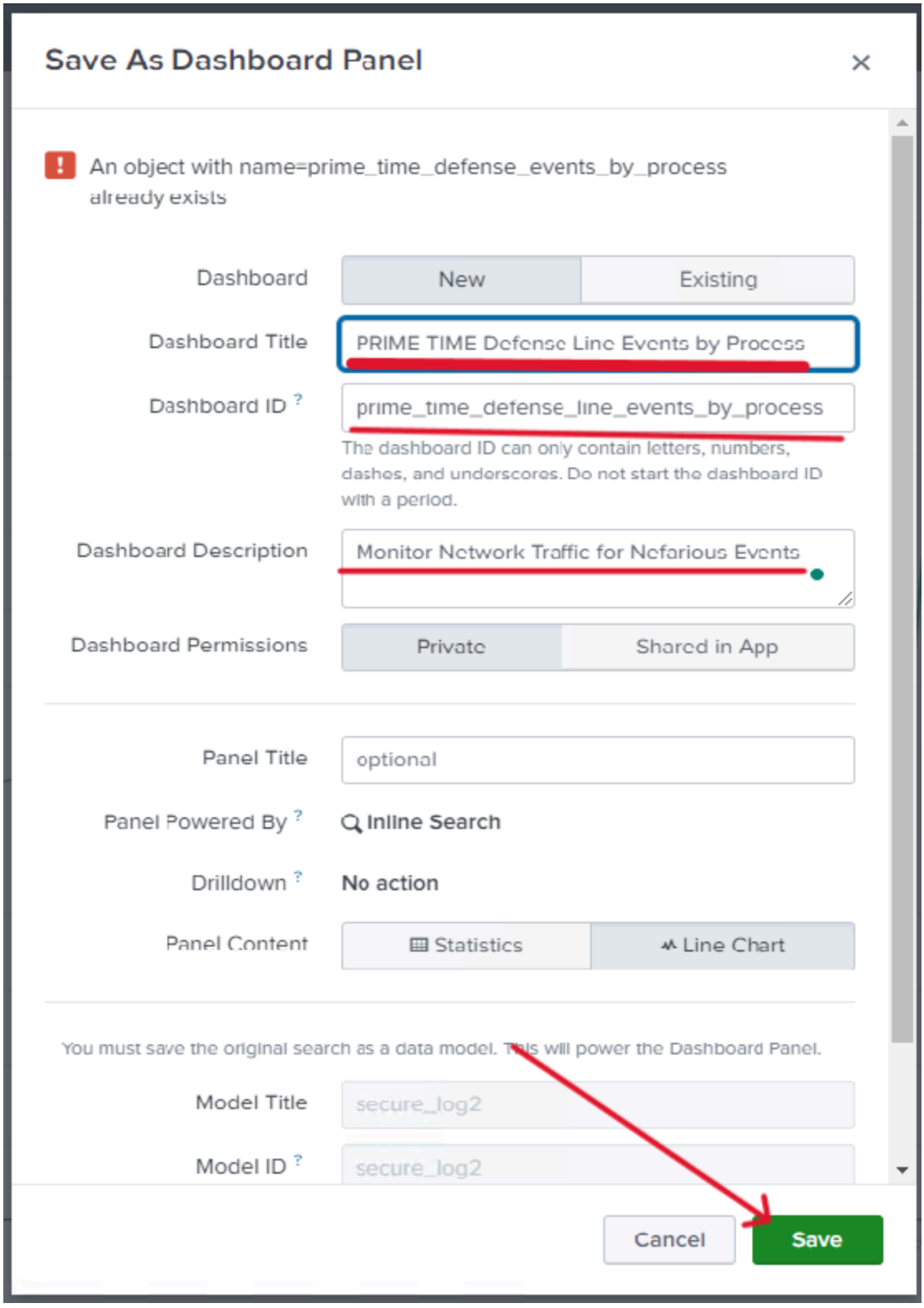

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
348,701 of 348,701 events matched
Line Chart
Time Range
Range
Last 24 hours
Filter

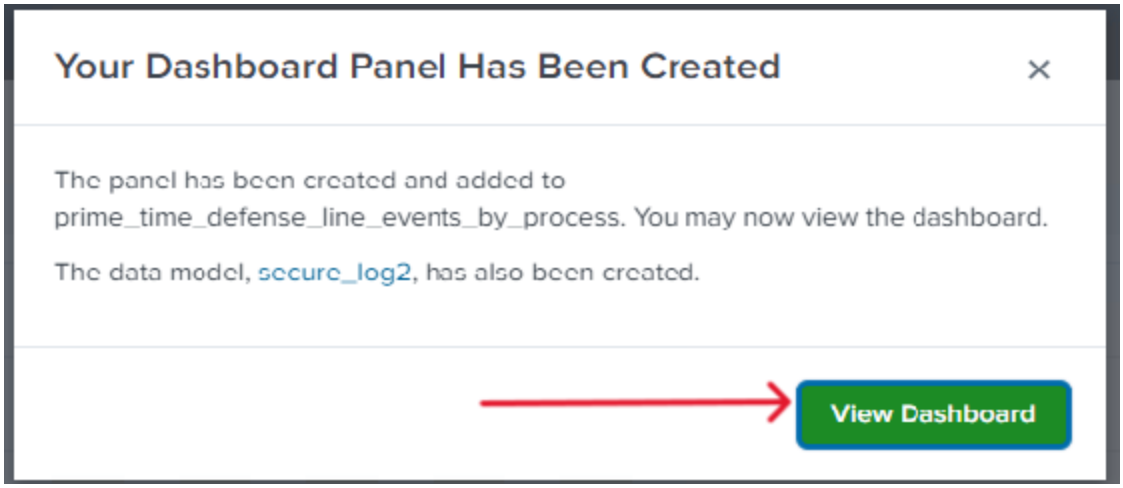

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,442,611 events (3/8/24 5:00:00.000 AM to 3/9/24 5:52:22.000
Time Range
Range
Last 24 hours
Filter
Add Filter
X-Axis (Time)
Label
show
Periods
Auto
Label Rotation
abc
Label Truncation
No
Y-Axis
Field
Count of 1709633971047
Label
show
Events
Scale
Linear
Log
Interval
optional
Min Value
optional
Max Value
optional
Color (Lines)
General

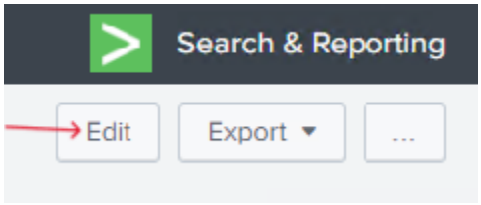

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Pivot
1,442,611 events (3/8/24 5:00:00.000 AM to 3/9/24 5:53:37.00
Time Range
Filter
X Axis (Time)
Y-Axis
Field
Count of 1709963397.1047
Label
show
Events
a Performance_state_type
pid
a Policy_ID
a Port
a Privileges
a process
a Process_Creation_Time
a Process_ID
a Process_Name
+ Add Color
General
Null Values
Multi-series Mode
Yes
No
Show Data Values
Off
On
Min/Max
10.0.0.6:8000/en-US/app/search/pivot?seedSid=1709963397.1047&earliest=-24h%40h&latest

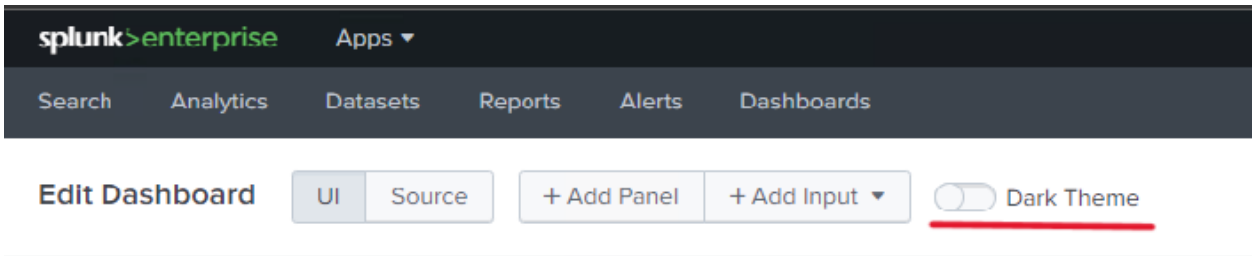

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
Save As...
Clear
Acceleration
1,442,611 events (3/8/24 5:00:00.000 AM to 3/9/24 5:55:02.000 AM)
Time Range
Range
Last 24 hours
Filter
Add Filter
X-Axis (Time)
Label
show
Periods
Auto
Label Rotation
Label Truncation
Yes
No
Y-Axis
Field
Count of 17099633971047
Label
show
Events
Scale
Linear
Log
Interval
optional
Min Value
optional
Max Value
optional
Color (Lines)
General
Events
65,000
60,000
55,000
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
6:00 AM
Fri Mar 8
2024
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
Sat Mar 9
2:00 AM
4:00 AM
_time
/sbin/init agent
CRON
NULL
accounts-daemon
acpid
amazon-ssm-agent,amazon-ssm-agent
apache2
apparmor.systemd
apport
cloud-init
cron
dbus-daemon
dhclient
elc_harvest_hostkeys
fwupdmgr
grub-common
hibinit-agent
kernel
lxd_activate
multipath
multipathd
networkd-dispatcher
passwd
polkitd
rsyslogd
snapd
splunk
sshd
sudo
systemd
systemd-fsck
systemd-logind
systemd-networkd
systemd-networkd-wait-online
systemd-resolved
systemd-sysctl
systemd-timesyncd
systemd-udevd
udevadm

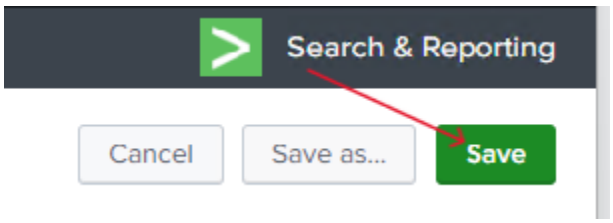

Settings
Activity
Help
Find
Search & Reporting
Save As...
Clear
Acceleration
Report
Dashboard Panel
/hibinit-agent
CRON
NULL
accounts-daemon
acpid
amazon-ssm-agent.amazon-ssm-agent
apachectl
apparmor.systemd
apport
cloud-init
cron
dbus-daemon
dhclient
eic_harvest_hostkeys
fwupdmgr
grub-common
hibinit-agent
kernel
lxd.activate
multipath
multipathd
networkd-dispatcher
passwd
polkitd
rsyslogd
snapd
splunk
sshd
sudo
systemd
systemd-fsck
systemd-logind
systemd-networkd
systemd-networkd-wait-online
systemd-resolved
systemd-sysctl
systemd-timesyncd
systemd-udevd
udevadm

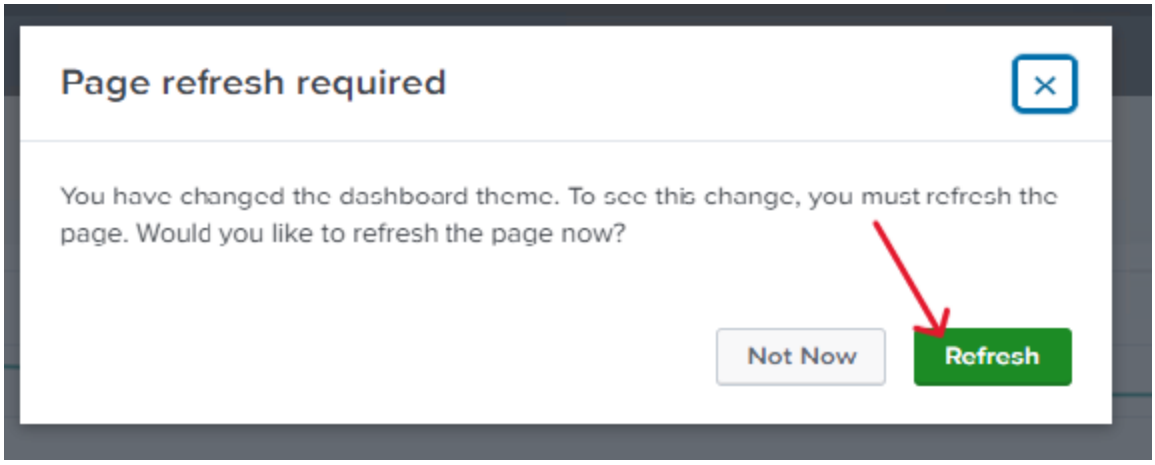

Save As Dashboard Panel
An object with name=prime_time_defense_events_by_process already exists
Dashboard
New
Existing
Dashboard Title
PRIME TIME Defense Line Events by Process
Dashboard ID
prime_time_defense_line_events_by_process
The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.
Dashboard Description
Monitor Network Traffic for Nefarious Events
Dashboard Permissions
Private
Shared in App
Panel Title
optional
Panel Powered By
Inline Search
Drilldown
No action
Panel Content
Statistics
Line Chart
You must save the original search as a data model. This will power the Dashboard Panel.
Model Title
secure_log2
Model ID
secure_log2
Cancel
Save

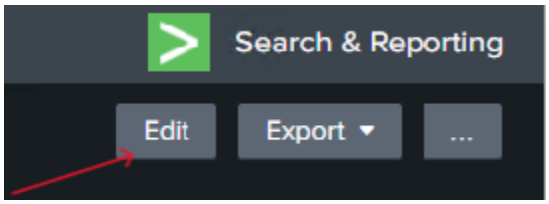

Your Dashboard Panel Has Been Created
The panel has been created and added to prime_time_defense_line_events_by_process. You may now view the dashboard.
The data model, secure_log2, has also been created.
View Dashboard

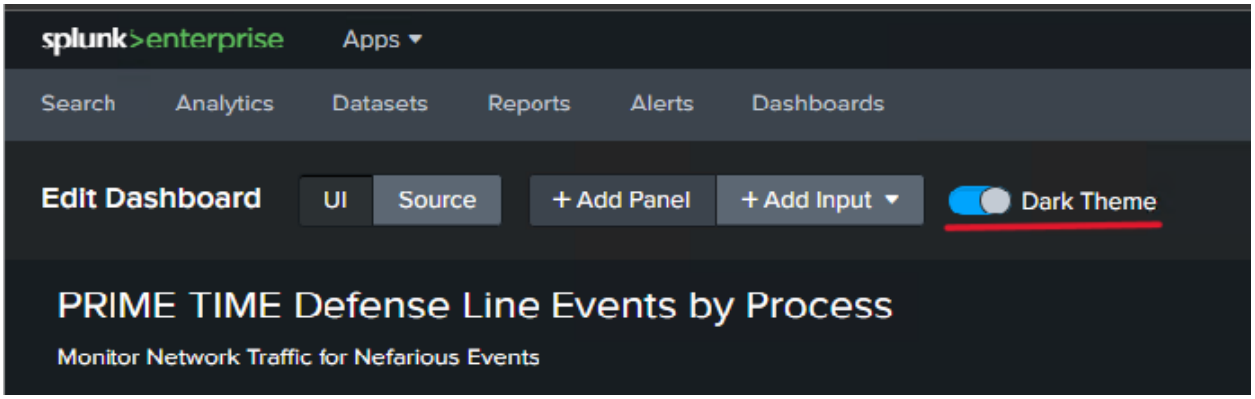

Search & Reporting
Edit
Export
...

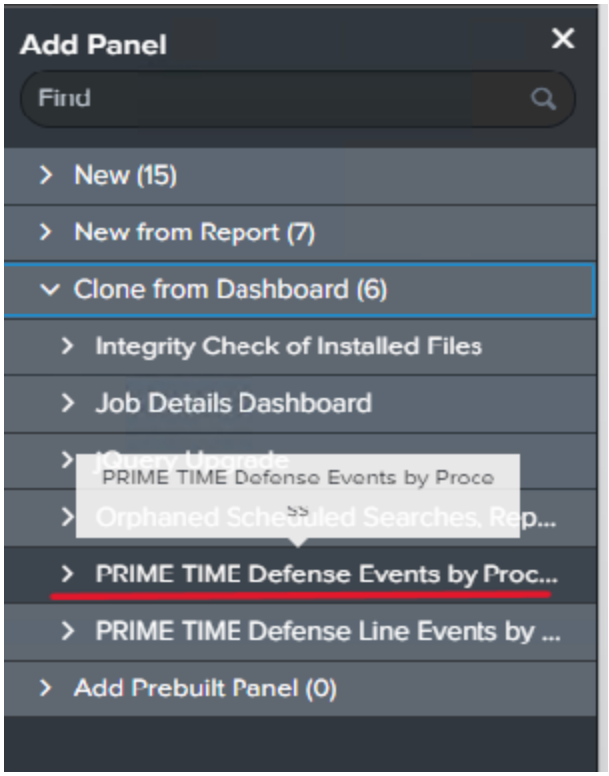

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
PRIME TIME Defense Line Events by Process
Monitor Network Traffic for Nefarious Events

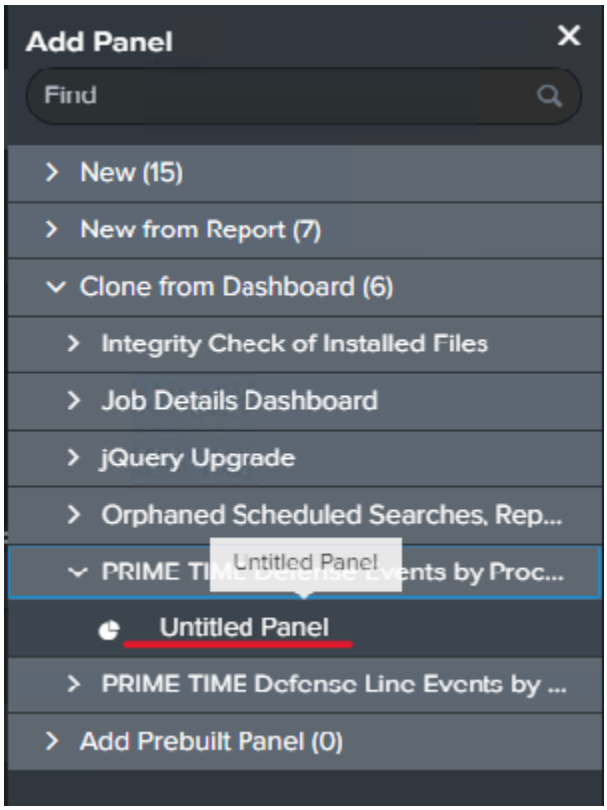

Search & Reporting
Cancel
Save as...
Save

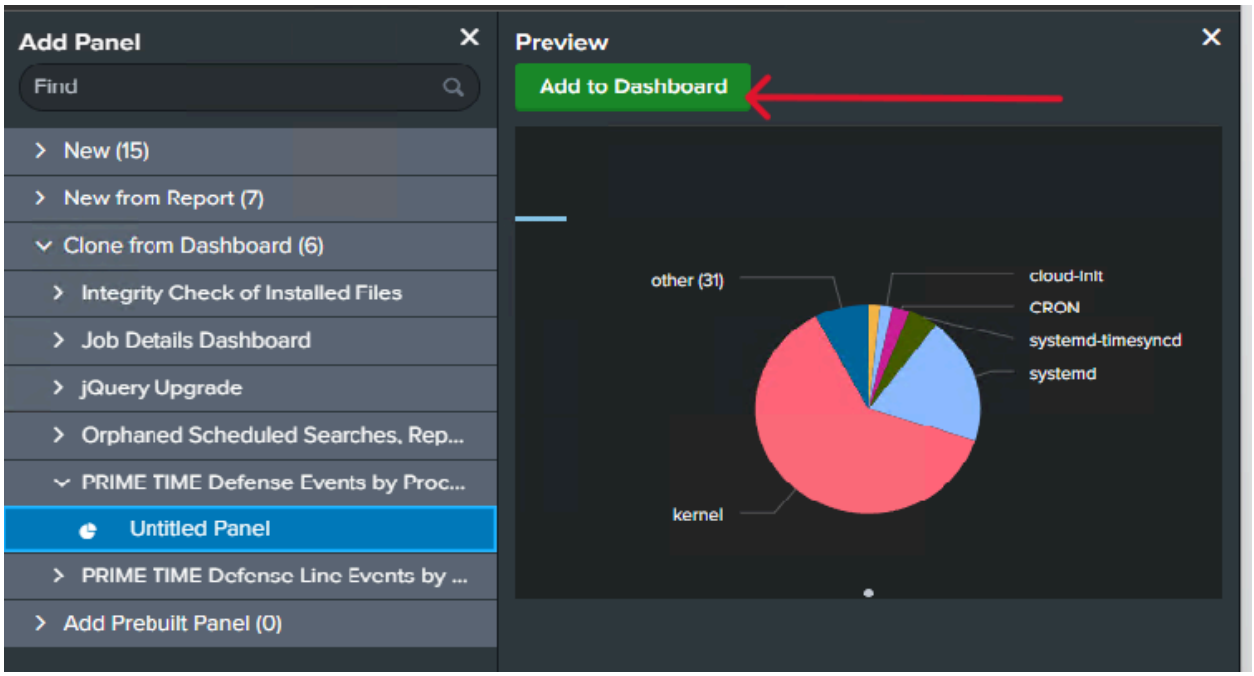

Page refresh required
You have changed the dashboard theme. To see this change, you must refresh the page. Would you like to refresh the page now?
Not Now
Refresh

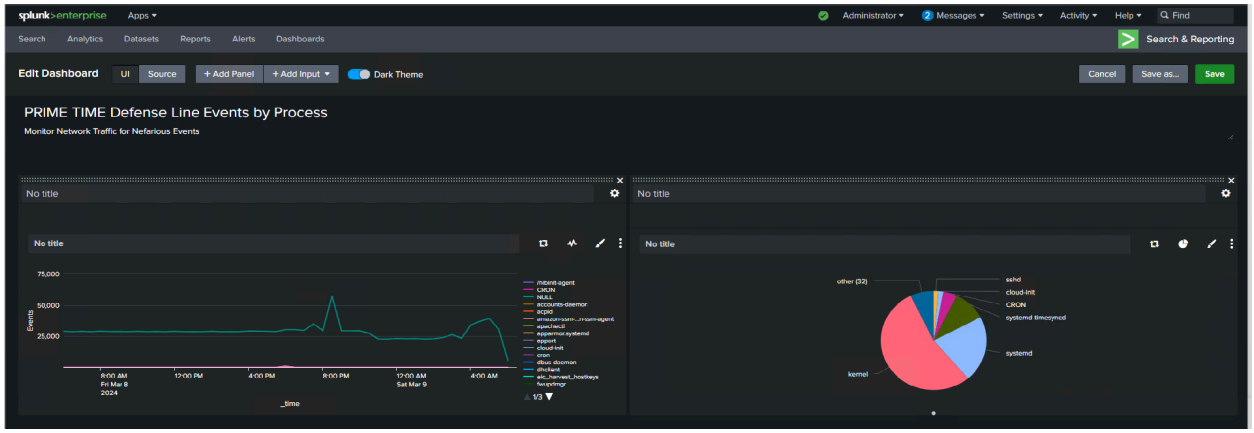

Search & Reporting
Edit
Export
...

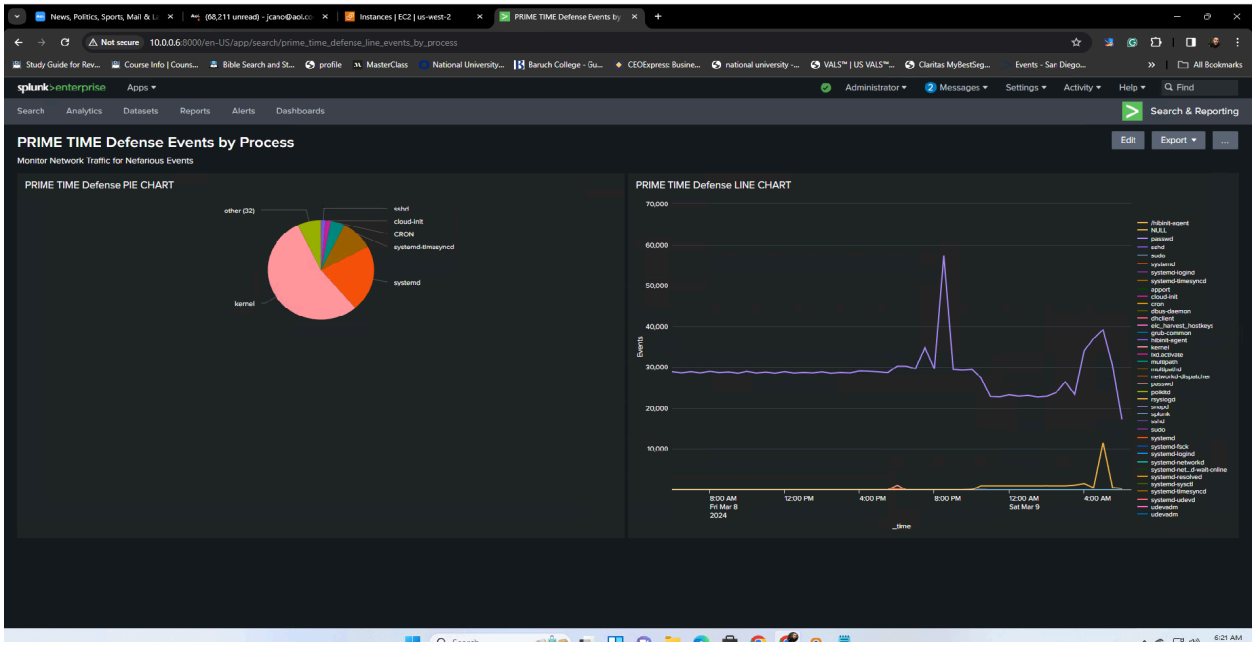

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
PRIME TIME Defense Line Events by Process
Monitor Network Traffic for Nefarious Events


Add Panel
Find
New (15)
New from Report (7)
Clone from Dashboard (6)
Integrity Check of Installed Files
Job Details Dashboard
PRIME TIME Defense Events by Proco
Orphaned Scheduled Searches, Rep...
PRIME TIME Defense Events by Proc...
PRIME TIME Defense Line Events by ...
Add Prebuilt Panel (0)

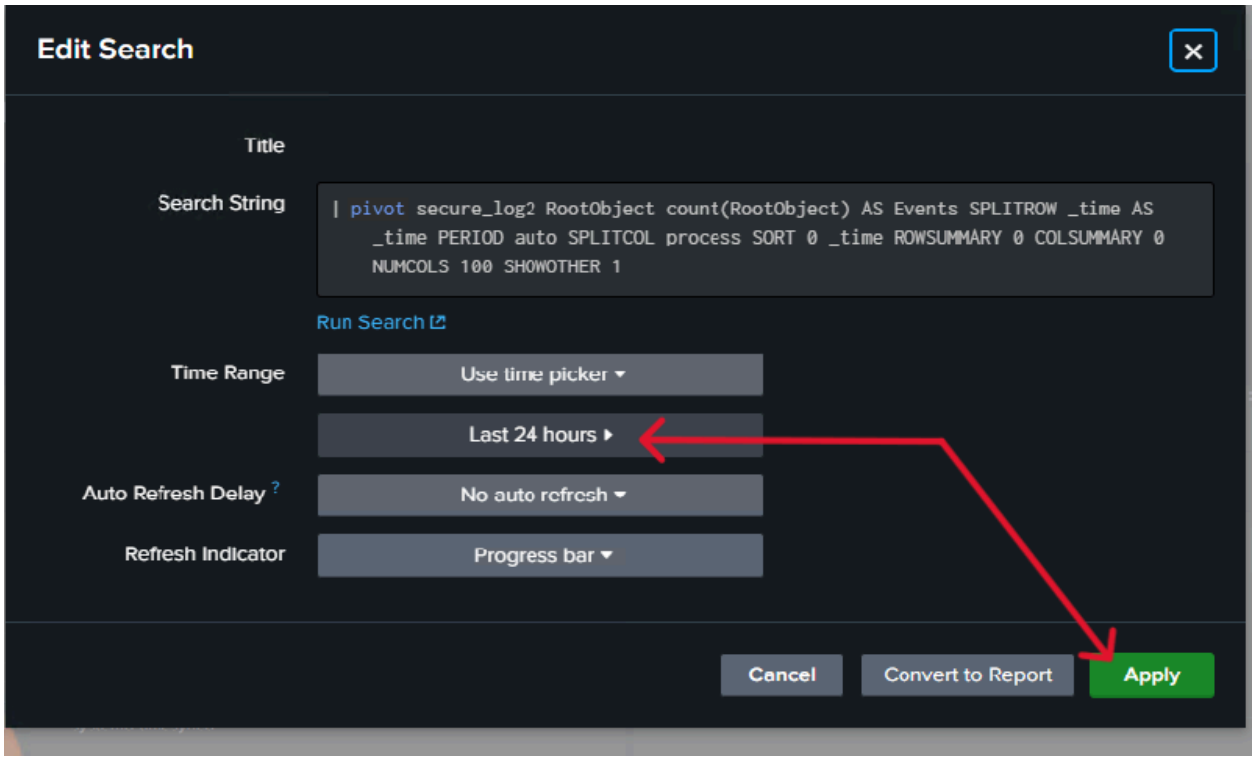

Add Panel
Find
New (15)
New from Report (7)
Clone from Dashboard (6)
Integrity Check of Installed Files
Job Details Dashboard
jQuery Upgrade
Orphaned Scheduled Searches, Rep...
Untitled Panel
Untitled Panel
PRIME TIME Defense Line Events by ...
Add Prebuilt Panel (0)

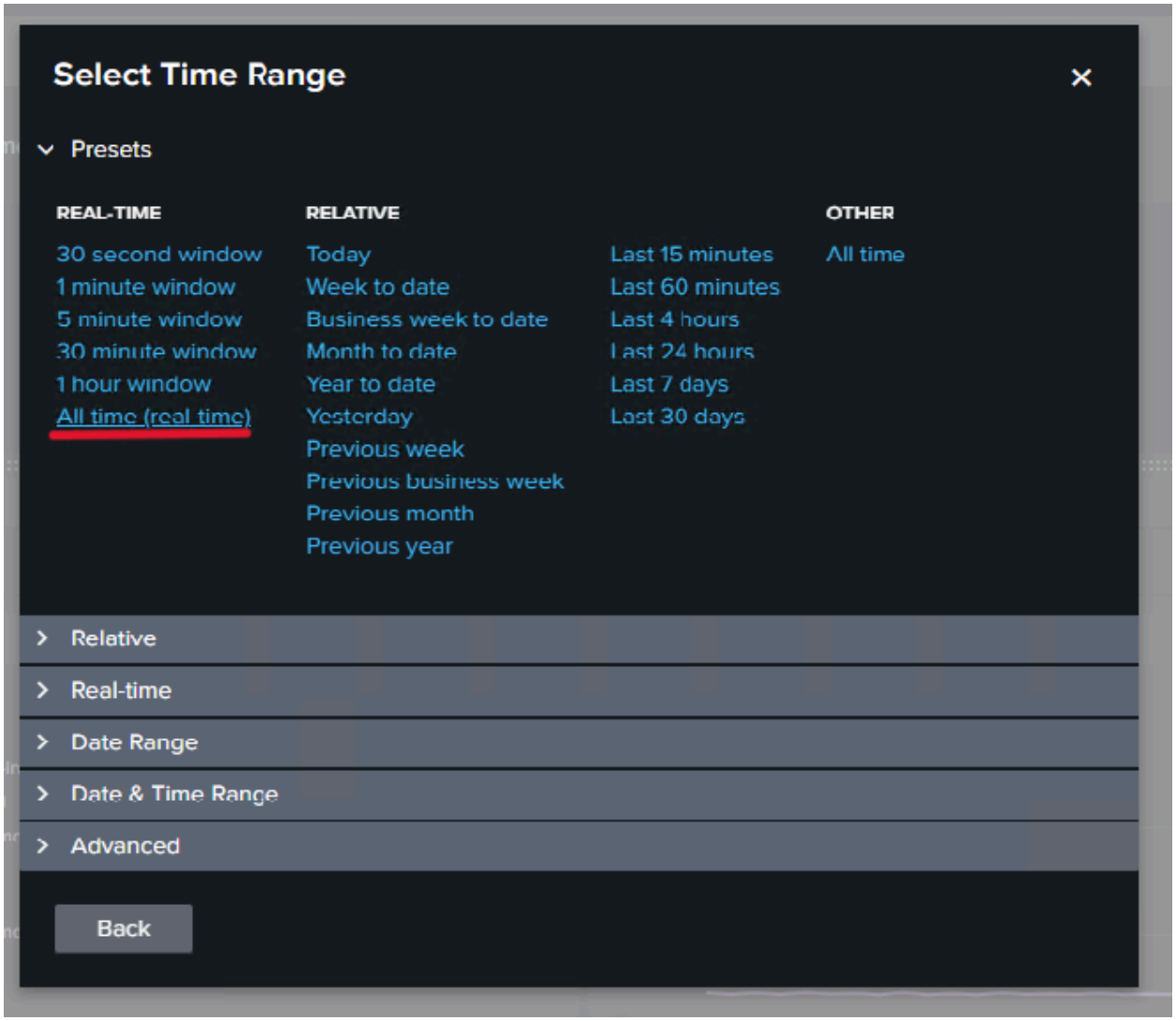

Add Panel
Find
New (15)
New from Report (7)
Clone from Dashboard (6)
Integrity Check of Installed Files
Job Details Dashboard
jQuery Upgrade
Orphaned Scheduled Searches, Rep...
PRIME TIME Defense Events by Proc...
Untitled Panel
PRIME TIME Defense Line Events by ...
Add Prebuilt Panel (0)
Preview
Add to Dashboard
other (31)
cloud-init
CRON
systemd-timesyncd
systemd
kernel

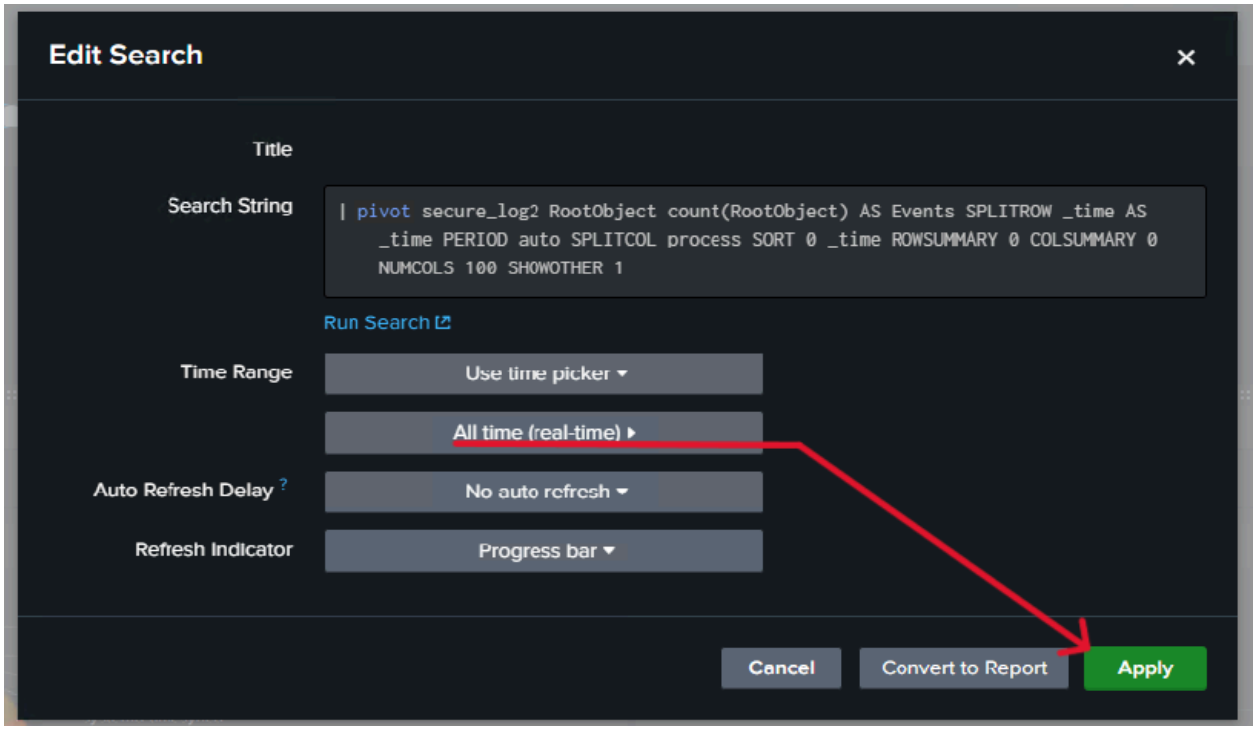

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
PRIME TIME Defense Line Events by Process
Monitor Network Traffic for Nefarious Events
No title
No title
No title
No title
75,000
50,000
25,000
Events
_time
other (32)
sshd
cloud-init
CRON
systemd timesynced
systemd
kernel

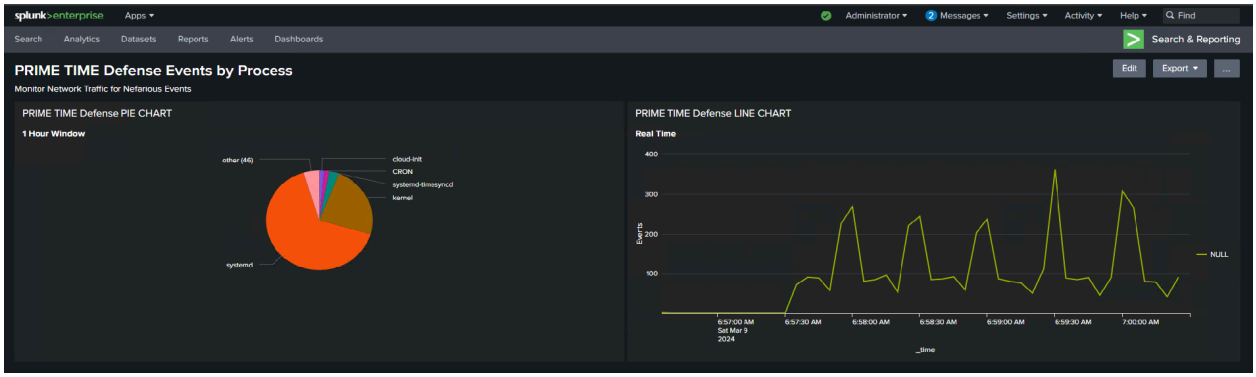

PRIME TIME Defense Events by Process
Monitor Network Traffic for Nefarious Events
PRIME TIME Defense PIE CHART
PRIME TIME Defense LINE CHART
Search & Reporting

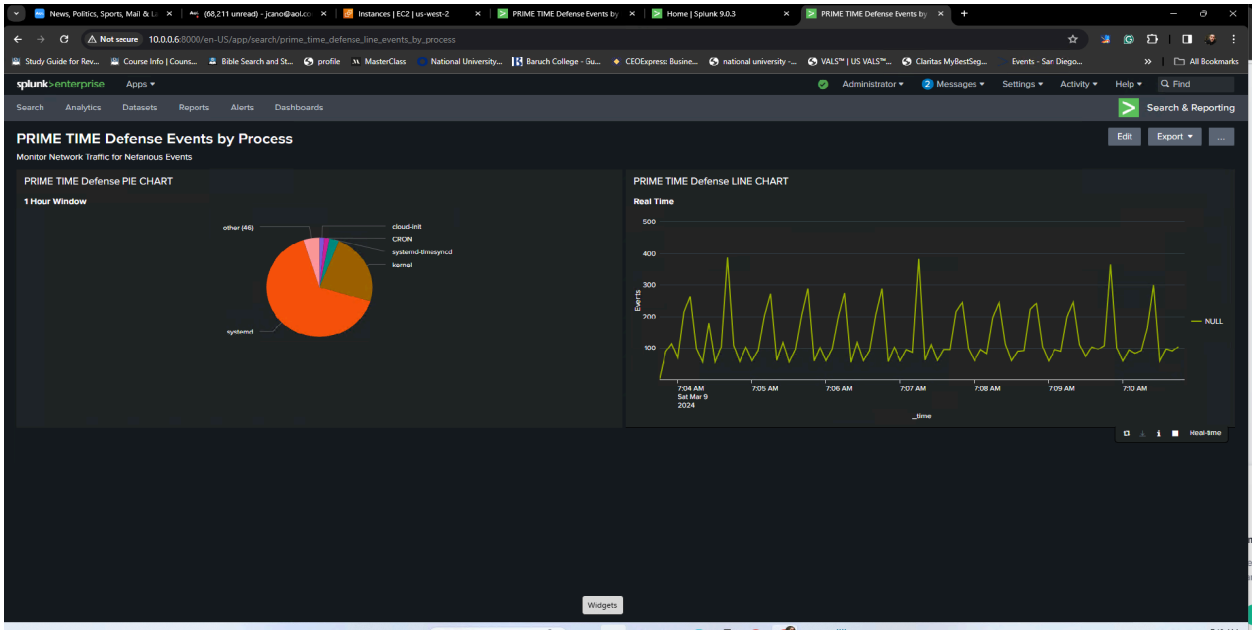

PRIME TIME Defense LINE CHART
Edit search
No title


Edit Search
Title
Search String
| pivot secure_log2 RootObject count(RootObject) AS Events SPLITROW _time AS _time PERIOD auto SPLITCOL process SORT 0 _time ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 100 SHOWOTHER 1
Run Search
Time Range
Use time picker
Last 24 hours
Auto Refresh Delay
No auto refresh
Refresh Indicator
Progress bar
Cancel
Convert to Report
Apply


Select Time Range
Presets
REAL-TIME
30 second window
1 minute window
5 minute window
30 minute window
1 hour window
All time (real time)
RELATIVE
Today
Week to date
Business week to date
Month to date
Year to date
Yesterday
Previous week
Previous business week
Previous month
Previous year
Last 15 minutes
Last 60 minutes
Last 4 hours
Last 24 hours
Last 7 days
Last 30 days
OTHER
All time
Relative
Real-time
Date Range
Date & Time Range
Advanced
Back


Edit Search
Title
Search String
| pivot secure_log2 RootObject count(RootObject) AS Events SPLITROW _time AS _time PERIOD auto SPLITCOL process SORT 0 _time ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 100 SHOWOTHER 1
Run Search
Time Range
Use time picker
All time (real-time)
Auto Refresh Delay
No auto refresh
Refresh Indicator
Progress bar
Cancel
Convert to Report
Apply


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
PRIME TIME Defense Events by Process
Monitor Network Traffic for Nefarious Events
Edit
Export
PRIME TIME Defense PIE CHART
1 Hour Window
other (46)
cloud-init
CRON
systemd-timesyncd
kernel
systemd
PRIME TIME Defense LINE CHART
Real Time
400
300
200
100
Events
NULL
6:57:00 AM Sat Mar 9 2024
6:57:30 AM
6:58:00 AM
6:58:30 AM
6:59:00 AM
6:59:30 AM
7:00:00 AM
_time



- **Searches**:
  - Predefine searches based on known attack patterns, indicators of compromise, and other relevant criteria to expedite the investigation process and response actions.
- **Lookup Tables**:
  - Use lookup tables to enrich log data with additional context, such as correlating IP addresses with device names or matching file hashes against known malicious files, enhancing the accuracy and effectiveness of analysis.
- **Field Extractions**:
  - Ensure accurate and efficient field extractions for critical data elements within log entries, facilitating more effective querying, filtering, and correlation of data across disparate sources.
- **Access Control**:
  - Implement robust access control measures within Splunk to ensure that only authorized personnel have access to sensitive data and configuration settings, preventing unauthorized access or modifications.
- **Backups**:
  - Establish regular backup routines for Splunk configurations and data, ensuring the ability to restore operations promptly in the event of system failure, data corruption, or other incidents.
- **Practice Runs**:
  - Conduct simulated attack scenarios or practice runs using mock data to validate the effectiveness of the Splunk configuration, identifying areas for improvement and ensuring readiness for actual cybersecurity events.
- **Documentation**:

    - Maintain comprehensive documentation and playbooks detailing the configuration, operation, and response procedures for the Splunk environment, providing a valuable resource for training, incident response, and continuity of operations.
- **Collaboration**:
    - Facilitate effective collaboration among cybersecurity team members, defining clear roles, responsibilities, and communication channels to ensure a coordinated and efficient response to detected threats or incidents.

5. Advanced Monitoring and Threat Detection

- **Real-time Searches and Alerts**: Optimize Splunk for immediate detection and alerting on potential threats by crafting searches that continuously monitor for indicators of compromise or suspicious patterns of behavior, ensuring alerts are actionable and prioritized based on severity.
- **Correlation Searches**: Develop sophisticated correlation searches that combine data from various sources, leveraging Splunk's correlation engine to identify complex attack patterns and multi-stage threats that might not be evident from single data points.
- **Anomaly Detection**: Implement anomaly detection techniques using Splunk's statistical and machine learning capabilities to identify outliers or deviations from established baselines, facilitating early detection of sophisticated attacks or insider threats.
- **User Behavior Analytics (UBA)**: If leveraging Splunk Enterprise Security, utilize the User Behavior Analytics (UBA) features to detect anomalies in user activities that deviate from normal patterns, identifying potential threats from compromised accounts or malicious insiders.

6. Forensic Investigation and Reporting

- **Incident Investigation**: Employ Splunk’s powerful search and analysis capabilities for in-depth forensic investigation of incidents, leveraging the ability to drill down into detailed log data, pivot based on specific fields, and trace the sequence of events across the attack lifecycle.
- **Timeline Analysis**: Utilize Splunk to construct detailed timelines of security events and incidents, enabling a comprehensive understanding of the attack progression, scope, and impact, which is crucial for effective response and mitigation strategies.
- **Scheduled Reports and PDF Exports**: Configure Splunk to automatically generate and distribute reports summarizing security incidents, trends, and overall posture, using scheduled PDF exports to provide stakeholders with regular, digestible updates on security metrics and incidents.

7. Leveraging Advanced Security Features and Customization

- **Splunk Enterprise Security (ES)**: For organizations with access to Splunk Enterprise Security, take advantage of its advanced security information and event management (SIEM) capabilities, including specialized dashboards, reports, and analysis tools tailored for comprehensive cybersecurity monitoring and response.
- **Custom Dashboards and Searches**: Customize Splunk dashboards and searches to specifically target the tactics, techniques, and procedures (TTPs) employed by the Red Team, creating

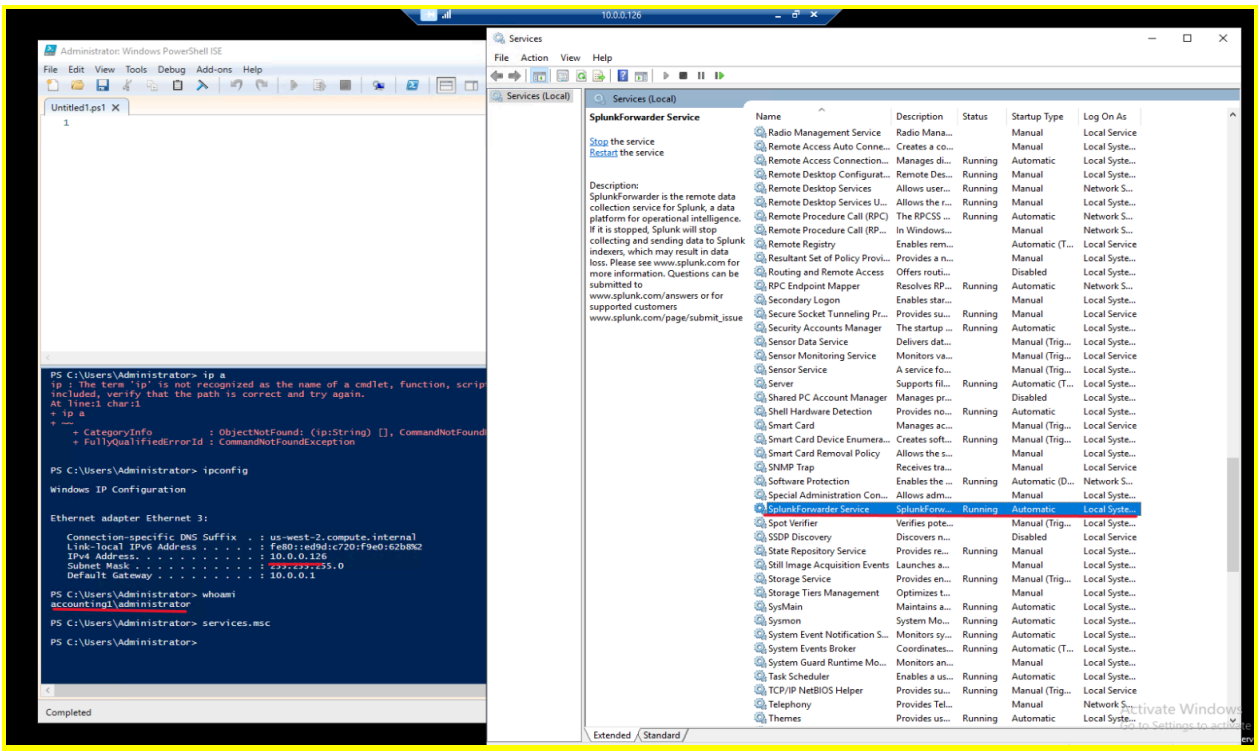
visualizations and alerts that highlight these activities in real-time, enhancing the effectiveness of the defense posture.

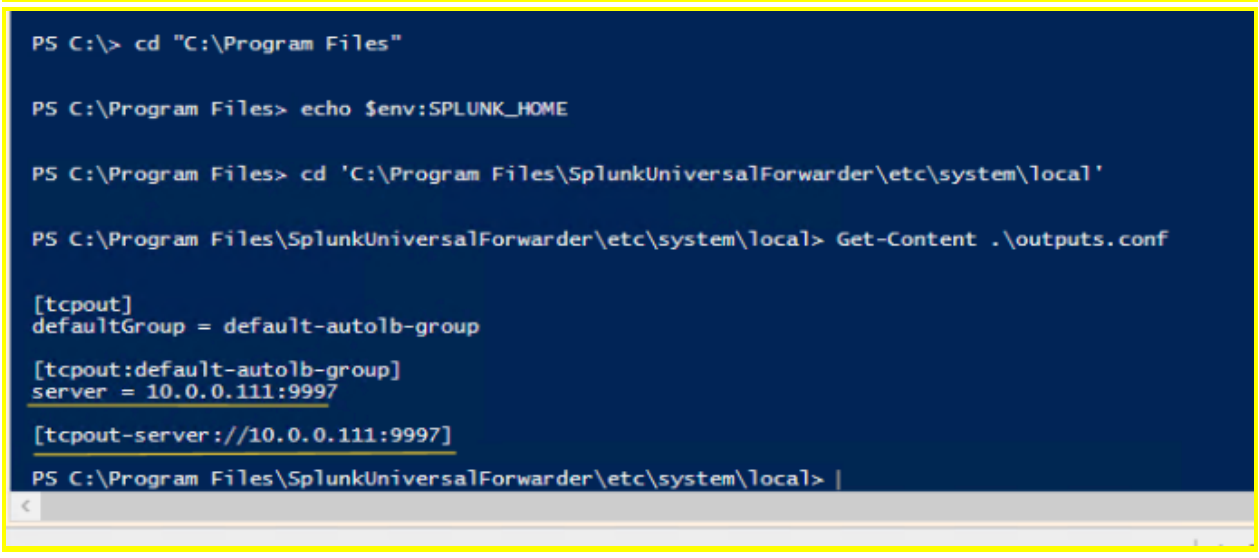
- **Splunk Apps**: Explore and integrate additional Splunk apps designed for specific cybersecurity use cases or to support defense against particular types of threats, leveraging the extensive Splunkbase repository to extend and enhance the capabilities of your Splunk environment for cybersecurity defense.

Conclusion

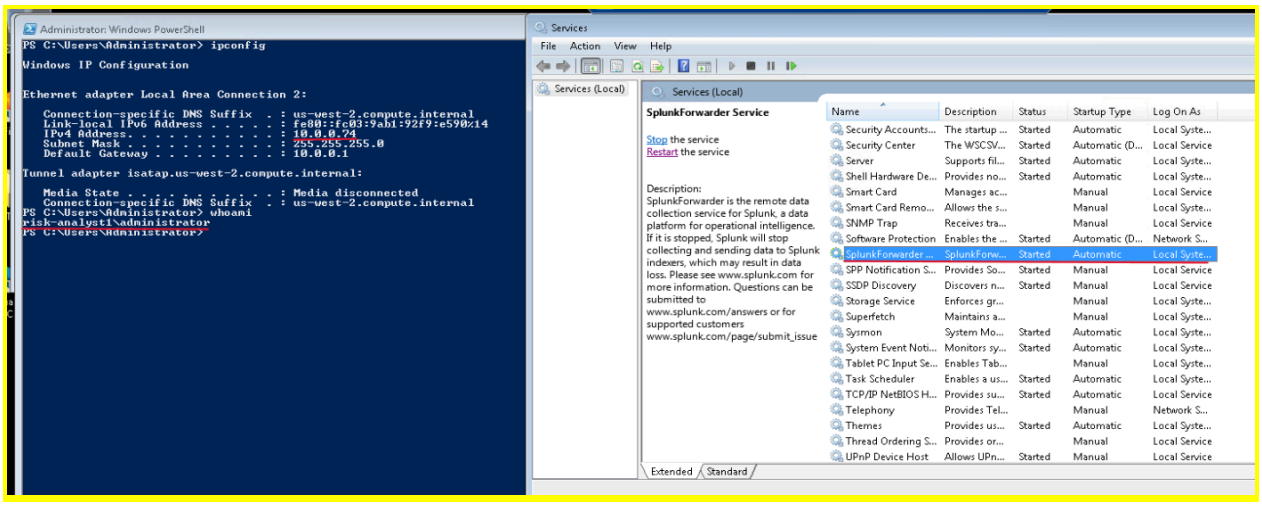
Utilizing Splunk effectively for cybersecurity defense involves a comprehensive setup encompassing data collection, real-time monitoring, advanced threat detection, forensic investigation, and continuous adaptation to evolving threats. Through diligent configuration, customization, and collaboration, cybersecurity teams can leverage Splunk's powerful capabilities to detect, respond to, and mitigate the activities of the Red Team, thereby safeguarding their organization's digital assets and infrastructure. Regular updates, practice drills, and leveraging the latest features and integrations available for Splunk will ensure that the defense mechanisms remain robust and effective against advanced threats.

Check your Network computer has Splunk Forwarder running to the correct Splunk IP:
Accounting 1:





Risk Analyst 1:

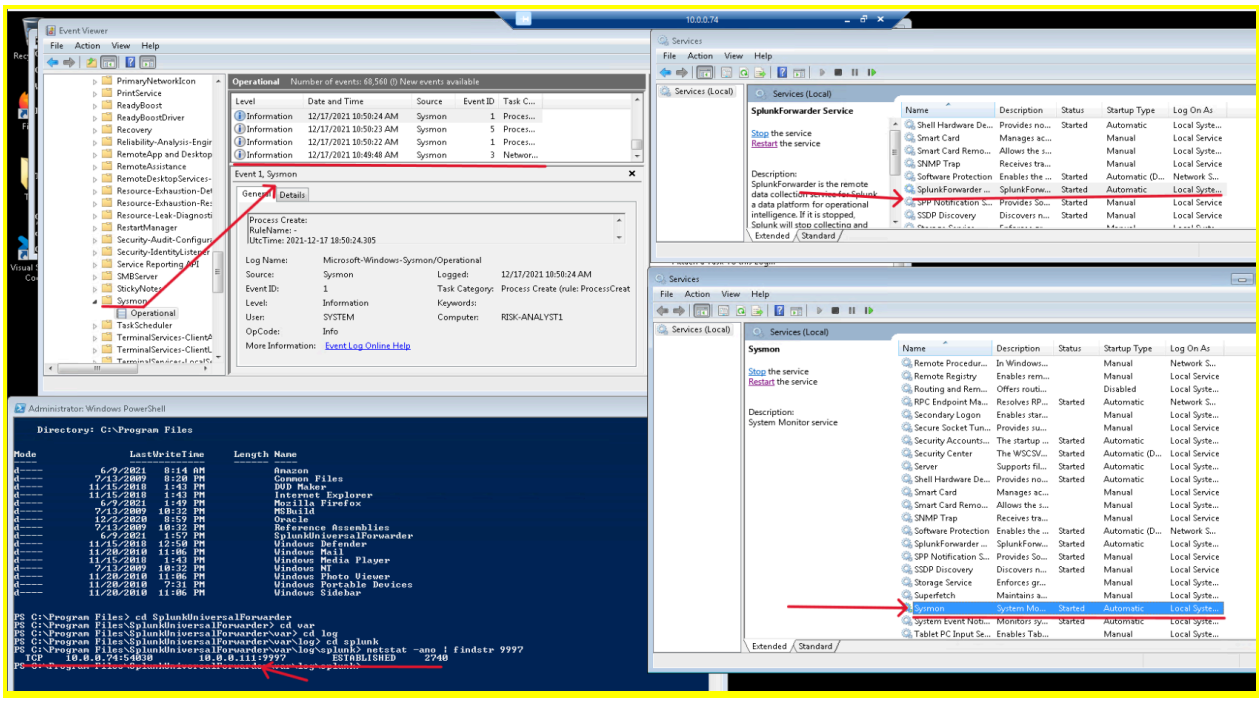



```
PS C:\Program Files> dir


    Directory: C:\Program Files


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d-----         6/9/2021   8:14 AM            Amazon
d-----        7/13/2009   8:20 PM            Common Files
d-----       11/15/2018   1:43 PM            DVD Maker
d-----       11/15/2018   1:43 PM            Internet Explorer
d-----         6/9/2021   1:49 PM            Mozilla Firefox
d-----        7/13/2009  10:32 PM            MSBuild
d-----        12/2/2020   8:59 PM            Oracle
d-----        7/13/2009  10:32 PM            Reference Assemblies
d-----         6/9/2021   1:57 PM            SplunkUniversalForwarder
d-----       11/15/2018  12:50 PM            Windows Defender
d-----       11/20/2010  11:06 PM            Windows Mail
d-----       11/15/2018   1:43 PM            Windows Media Player
d-----        7/13/2009  10:32 PM            Windows NT
d-----       11/20/2010  11:06 PM            Windows Photo Viewer
d-----       11/20/2010   7:31 PM            Windows Portable Devices
d-----       11/20/2010  11:06 PM            Windows Sidebar


PS C:\Program Files> cd SplunkUniversalForwarder
PS C:\Program Files\SplunkUniversalForwarder> cd var
PS C:\Program Files\SplunkUniversalForwarder\var> cd log
PS C:\Program Files\SplunkUniversalForwarder\var\log> cd splunk
PS C:\Program Files\SplunkUniversalForwarder\var\log\splunk> netstat -ano | findstr 9997
  TCP    10.0.0.74:54030        10.0.0.111:9997        ESTABLISHED     2740
PS C:\Program Files\SplunkUniversalForwarder\var\log\splunk>
```


Event Viewer
File Action View Help
Operational Number of events: 68,560 (!) New events available
Level Date and Time Source Event ID Task C...
Information 12/17/2021 10:50:24 AM Sysmon 1 Proces...
Information 12/17/2021 10:50:23 AM Sysmon 5 Proces...
Information 12/17/2021 10:50:22 AM Sysmon 1 Proces...
Information 12/17/2021 10:49:48 AM Sysmon 3 Networ...
Event 1, Sysmon
General Details
Process Create:
RuleName: -
UtcTime: 2021-12-17 18:50:24.305
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 12/17/2021 10:50:24 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreat
Level: Information
Keywords:
User: SYSTEM
Computer: RISK-ANALYST1
OpCode: Info
More Information: Event Log Online Help
Administrator: Windows PowerShell
Directory: C:\Program Files
Mode LastWriteTime Length Name
d----- 6/9/2021 8:14 AM Amazon
d----- 7/13/2009 8:20 PM Common Files
d----- 11/15/2018 1:43 PM DUD Maker
d----- 11/15/2018 1:43 PM Internet Explorer
d----- 6/9/2021 1:49 PM Mozilla Firefox
d----- 7/13/2009 10:32 PM MSBuild
d----- 12/2/2020 8:59 PM Oracle
d----- 7/13/2009 10:32 PM Reference Assemblies
d----- 6/9/2021 1:57 PM SplunkUniversalForwarder
d----- 11/15/2018 12:50 PM Windows Defender
d----- 11/20/2010 11:06 PM Windows Mail
d----- 11/15/2018 1:43 PM Windows Media Player
d----- 7/13/2009 10:32 PM Windows NT
d----- 11/20/2010 11:06 PM Windows Photo Viewer
d----- 11/20/2010 7:31 PM Windows Portable Devices
d----- 11/20/2010 11:06 PM Windows Sidebar
PS C:\Program Files> cd SplunkUniversalForwarder
PS C:\Program Files\SplunkUniversalForwarder> cd var
PS C:\Program Files\SplunkUniversalForwarder\var> cd log
PS C:\Program Files\SplunkUniversalForwarder\var\log> cd splunk
PS C:\Program Files\SplunkUniversalForwarder\var\log\splunk> netstat -ano | findstr 9997
TCP 10.0.0.74:54030 10.0.0.111:9997 ESTABLISHED 2740
Services
File Action View Help
Services (Local)
SplunkForwarder Service
Stop the service
Restart the service
Description:
SplunkForwarder is the remote data collection service for Splunk a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and
Name Description Status Startup Type Log On As
Shell Hardware De... Provides no... Started Automatic Local Syste...
Smart Card Manages ac... Manual Local Service
Smart Card Remo... Allows the s... Manual Local Syste...
SNMP Trap Receives tra... Manual Local Service
Software Protection Enables the ... Started Automatic (D... Network S...
SplunkForwarder ... SplunkForw... Started Automatic Local Syste...
SPP Notification S... Provides So... Started Manual Local Service
SSDP Discovery Discovers n... Started Manual Local Service
Extended Standard
Services
File Action View Help
Services (Local)
Sysmon
Stop the service
Restart the service
Description:
System Monitor service
Name Description Status Startup Type Log On As
Remote Procedur... In Windows... Manual Network S...
Remote Registry Enables rem... Manual Local Service
Routing and Rem... Offers routi... Disabled Local Syste...
RPC Endpoint Ma... Resolves RP... Started Automatic Network S...
Secondary Logon Enables star... Manual Local Syste...
Secure Socket Tun... Provides su... Manual Local Service
Security Accounts... The startup ... Started Automatic Local Syste...
Security Center The WSCSV... Started Automatic (D... Local Service
Server Supports fil... Started Automatic Local Syste...
Shell Hardware De... Provides no... Started Automatic Local Syste...
Smart Card Manages ac... Manual Local Service
Smart Card Remo... Allows the s... Manual Local Syste...
SNMP Trap Receives tra... Manual Local Service
Software Protection Enables the ... Started Automatic (D... Network S...
SplunkForwarder ... SplunkForw... Started Automatic Local Syste...
SPP Notification S... Provides So... Started Manual Local Service
SSDP Discovery Discovers n... Started Manual Local Service
Storage Service Enforces gr... Manual Local Syste...
Superfetch Maintains a... Manual Local Syste...
Sysmon System Mo... Started Automatic Local Syste...
System Event Noti... Monitors sy... Started Automatic Local Syste...
Tablet PC Input Se... Enables Tab... Manual Local Syste...
Extended Standard